

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
SHERMAN DIVISION

THE TRANSPARENCY PROJECT,

Plaintiff,

V.

U.S. DEPARTMENT OF JUSTICE, et al.,

Defendants.

Civil Action No. 4:20CV467

JUDGE SEAN D. JORDAN

DECLARATION OF KEVIN G. TIERNAN

I, Kevin G. Tiernan, do hereby state and declare as follows:

1. I am the Supervisory Records Manager in the Records and Freedom of Information Act (“FOIA”) Unit in the National Security Division (“NSD”) of the United States Department of Justice (“DOJ” or “Department”).

2. My duties as Supervisory Records Manager of the Records and FOIA Unit include the supervision of NSD's execution of its obligations under FOIA, 5 U.S.C. § 552.

3. The statements herein are based on my personal knowledge of plaintiff's FOIA request and on reports made to me by NSD personnel and other information I acquired while performing my official duties. I submit this declaration in my official capacity; in that capacity, if called as a witness, I would be competent to testify to the information available to the NSD.

4. This declaration serves as a supplement to the original declaration filed in this matter by Patrick Findlay on behalf of NSD, dated February 2, 2022. A copy of NSD's initial declaration is attached hereto as Exhibit A.

5. As stated in the aforementioned declaration, NSD FOIA assigned Plaintiff's FOIA request dated June 15, 2020, tracking number NSD 20-333, and assigned Plaintiff's FOIA request dated June 18, 2020 tracking number NSD 20-338.

6. The search for records responsive to NSD 20-333 consisted of an initial search of former Assistant Attorney General John Demers' email account and personal drive. This initial search relied on the terms: "60 minutes"; "DNC emails"; "Seth Conrad Rich"; "Aaron Nathan Rich"; "DNC emails" & "2016"; "DNC emails" & "wikileaks"; "Debbie Wasserman-Shultz" & "Imran Awan, Abid Awan, Jamal Awan, Hina Alvi, Rao Abbas"; "Congress" & "Imran Awan, Abid Awan, Jamal Awan, Hina Alvi, Rao Abbas"; "Debbie Wasserman-Shultz" & "Pakistan" and identified one responsive record. NSD's interim response produced that record in part.

7. The subject matter of the request and initial results led NSD FOIA to conclude that additional responsive records, if any, were likely to be housed in the Office of the Assistant Attorney General (OAAG) and in NSD's Counterintelligence and Export Control Section (CES). As such, NSD FOIA conducted additional searches, using the same terms, of the email accounts, personal drives and shared drives of line attorneys and supervisors identified as possible custodians of potentially responsive records in OAAG and CES. These additional searches identified responsive records. NSD's final response produced the responsive records in part.

8. The search for records responsive to item two of NSD 20-338 consisted of a search of the records of CES regarding the investigation and prosecution of former Director of the Central

Intelligence Agency David Petraeus. Based on the subject of this item of the request, NSD FOIA determined that CES was the section that would have responsive records if there were any.

Accordingly, NSD FOIA coordinated with the case manager in the CES responsible for maintaining records for cases involving CES. The case manager searched the CES shared drives and coordinated local, manual searches of line attorneys' email accounts and personal drives.

NSD's search identified records responsive to the request. NSD's final response produced the responsive records in full.

I certify, pursuant to 28 U.S.C. § 1746, under penalty of perjury, that the foregoing is true and correct.

Kevin G. Tiernan

Executed on this 27th day of September 2022.

EXHIBIT A

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
SHERMAN DIVISION

THE TRANSPARENCY PROJECT,	§	
	§	
Plaintiff,	§	CIVIL ACTION No. 4:20CV467
	§	
v.	§	
	§	
U.S. DEPARTMENT OF JUSTICE, et al.,	§	JUDGE SEAN D. JORDAN
	§	
Defendants.	§	

DECLARATION OF PATRICK N. FINDLAY

I, Patrick N. Findlay, do hereby state and declare as follows:

1. I am the General Counsel of the National Security Division (NSD) of the United States Department of Justice (“DOJ” or the “Department”). I lead the Office of General Counsel (“OGC”), which is the successor organization to NSD’s former Office of Strategy Management and Development (“OSMD”). NSD is a component of the Department. *See* 72 Fed. Reg. 10064 (Mar. 7, 2007). I have served as the General Counsel of NSD since March of 2020 and was previously the Acting Chief of OSMD from July 2018 until its dissolution and replacement with the OGC in March of 2020. Prior to serving as the Acting Chief, I was a Special Counsel in OSMD from June 2016 to July 2018. Prior to my positions with NSD, I served as an Associate General Counsel for the Federal Bureau of Investigation (“FBI”) from July 2012 until June 2016.

2. The Records and Freedom of Information Act Unit (“NSD FOIA”) is a constituent part of OGC and is responsible for responding to requests for access to NSD records and information pursuant to the Freedom of Information Act (“FOIA”), *codified at* 5 U.S.C. § 552, as well as processing the NSD records which are responsive to FOIA requests received by other parts of the Executive Branch.

3. As NSD General Counsel, I have been delegated Top Secret Original Classification Authority (“OCA”) by the Attorney General of the United States. *See* Exec. Order No. 13526 § 1.3(c) (Dec. 29, 2009).

4. Through the exercise of my official duties, I have become familiar with this action and the underlying FOIA requests at issue. The statements contained herein are based upon my personal knowledge of the subject of the FOIA requests, as well as information provided to me in the course of my official duties.

5. I submit this declaration in support of the Department’s motion for summary judgment in this proceeding.

Plaintiff’s FOIA Requests and NSD’s Responses

6. Related to this litigation, NSD FOIA received several FOIA requests from Plaintiff by electronic filing. The first request was dated October 26, 2018, a copy of which is attached hereto as Exhibit A. The second request was dated June 11, 2020, a copy of which is attached hereto as Exhibit B. The third request was dated June 15, 2020, a copy of which is attached hereto as Exhibit C. The fourth request, through which the Plaintiff sought the same records requested via the request of October 26, 2018, was dated June 18, 2020, a copy of which is attached hereto as Exhibit D.

7. On September 2, 2020, NSD FOIA responded to the June 11, 2020, request indicating that the request had been assigned tracking number NSD 20-341. A copy of this NSD response is attached as Exhibit E. In this response, NSD FOIA further informed Plaintiff that it does not maintain FBI records and sought clarification. NSD FOIA went on to note that, as such, if NSD FOIA did not receive a response within 30 days, the request would be administratively closed.

NSD FOIA did not receive such a response, and NSD 20-341 was administratively closed accordingly.

8. On November 5, 2020, NSD FOIA responded to the June 15, 2020, request, indicating that the request had been assigned tracking number NSD 20-333. A copy of this NSD response is attached as Exhibit F.

9. NSD FOIA issued an interim response to NSD 20-333 on March 9, 2021, releasing one 40-page record in part, with redactions made per 5 U.S.C. § 552(b)(6). A copy of this NSD response is attached as Exhibit G.

10. NSD FOIA issued a final response to NSD 20-333 on August 30, 2021, whereby it released one record that was 149 pages in length, with redactions made pursuant to 5 U.S.C. § 552(b)(6). A copy of this NSD response is attached as Exhibit H.

11. On November 16, 2021, NSD FOIA issued a final response to the request dated June 18, 2020, indicating that the request had been assigned tracking number NSD 20-338 and releasing one record in full as responsive to part two of the request. A copy of this NSD response is attached as Exhibit I. Further, in this response, NSD FOIA declined to confirm or deny the existence of records responsive to part one of this request, a so-called *Glomar* response, per 5 U.S.C. § 552(b)(1). Finally, NSD FOIA noted that it had referred one additional record to a different component of the Department for direct response to Plaintiff.

NSD's *Glomar* Response

12. Part one of NSD 20-338 sought the following records:

I request the opportunity to view all documents, records, communications and/or other tangible evidence reflecting or pertaining to surveillance of Edward Butowsky of Texas or Matt Couch of Arkansas. The term "surveillance" includes, but is not limited to, any attempt to hack into the computers, phones, other electronic devices, and/or online accounts of Mr.

Butowsky or Mr. Couch. If any information obtained by surveillance was relayed to third parties, that information should be produced for inspection.

13. Based on its context, NSD FOIA interpreted the request as seeking NSD records regarding surveillance that, should they exist, would have been authorized under the *Foreign Intelligence Surveillance Act of 1978* (FISA), codified at 50 U.S.C. § 1801, *et seq.* As such, NSD FOIA asserted and continues to assert, a *Glomar* response to item one of the request pursuant to FOIA Exemption 1 as further explained below.

14. As background, I note that because much of NSD's work is of a classified nature, NSD FOIA frequently asserts Exemption 1, protecting properly classified information from disclosure in response to FOIA requests.¹ Information in NSD records is frequently, though not exclusively, classified under section 1.4(c) of Executive Order 13526 which covers intelligence activities, sources, and methods.² In circumstances where a confirmation that responsive records exist would disclose a classified fact, such as with item one in this request, NSD's usual practice is to assert a *Glomar* response, thereby neither confirming nor denying the existence of information that would disclose or suggest any such fact pursuant to FOIA Exemption 1 and section 3.6(a) of Executive Order 13526.³

¹ See 5 U.S.C. § 552(b)(1) (“(A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant such Executive order.”)

² Section 1.4 protects as classified information that “could reasonably be expected to cause identifiable or describable damage to the national security” with subsection c covering “intelligence activities (including covert action), intelligence sources or methods, or cryptology.”

³ “An agency may refuse to confirm or deny the existence or nonexistence of requested records whenever the fact of their existence or nonexistence is itself classified under this order or its predecessors.” Exec. Order No. 13526 § 3.6(a).

15. As further background, I note that section 2.2 of Executive Order 13526 provides for the derivative classification of National Security Information (NSI) by individuals who are not OCAs, including staff of NSD FOIA, through the use of classification guidance. *The United States Department of Justice, National Security Information, Classification Guide* (Ver. 2) (August 22, 2019) (“NSICG”) is one such example. NSICG sets forth derivative classification guidance for certain information regularly encountered in NSD FOIA’s work.

16. Several enumerated categories of information in the NSICG, designated for protection under section 1.4(c) of Executive Order 13526, would apply to records responsive to part one of this request, if any such records were to exist. Specifically, such items would be classified under the NSICG as “an investigative technique requiring a FISA court order or other FISA authorized collection,” *see* NSICG, Table 1.10, Item No.INV-4 (a), or because “[t]he fact that a FISA court order or other FISA authorized collection was applied for or obtained in a specific case,” *see* NSICG, Table 1.10, Item No.INV-8. Consistent with the longstanding treatment of FISA collection as classified, NSD FOIA determined that any FISA-related information responsive to part one of the request would be classified, if it existed, absent some countervailing public disclosure or other action leading to declassification.

17. As an OCA, I confirm that the guidance provided in the NSICG is appropriate in requiring the classification of FISA-related records responsive to part one of Plaintiff’s request, should they exist, as they would implicate section 1.4 (c) of Executive Order 13526. This is because such disclosure would cause harm to national security as it could permit hostile intelligence services to use FOIA to acquire information about United States intelligence investigations. Once a particular source or method, or the fact of its use in a particular situation, is disclosed, its continued usefulness may be degraded. If NSD were to indicate that it maintains

responsive information, such confirmation would provide intelligence analysts of foreign intelligence services with individual pieces of information that could be compiled into a catalogue of FISA activities. Intelligence services and other adversaries could use these disclosures to gain insight into which intelligence agents operating in this country were known to the U.S. Government and which were not. Further, this information could be used to deploy counterintelligence assets against the U.S. Government thereby impairing U.S. intelligence collection.

18. Conversely, revealing the absence of responsive records pertaining to particular individuals would tend to indicate that persons within the scope of the request were not targets of surveillance conducted pursuant to FISA. That fact could be extremely valuable to foreign powers and hostile intelligence services who could use it to carry out intelligence activities with some comfort that the U.S. Government is either not monitoring certain people and may not even suspect them or otherwise is not concerned with their activities.

19. As a result, to protect critical intelligence information and minimize the harm to national security, NSD necessarily asserts a *Glomar* response to requests for information pertaining to operational FISA work. Any such records, were they to exist, would relate to intelligence collection overseen, though not undertaken, by NSD. The existence of such operations is properly classified under section 1.4(c) of Executive Order 13526. Thus, NSD must refuse to confirm or deny whether or not such records exist.

20. Further, to be credible and effective, absent highly unusual circumstances, NSD must use the *Glomar* response consistently in all cases where the existence of records responsive to a FOIA request is a classified fact, as it is here, including instances in which NSD does not possess records responsive to a particular request. If NSD were to invoke a *Glomar* response only

when it actually possessed responsive records, the *Glomar* response would be interpreted as an admission that responsive records exist. This practice would reveal the very information that NSD must protect in the interest of national security. An admission of the fact that NSD was in possession of particular records relating to specific FISA-authorized surveillance targets would provide hostile foreign powers with access to additional, operationally valuable information about hypothetical United States intelligence investigations and allow those powers to subvert those same hypothetical investigations. Similarly, if NSD were to make clear to the public via a response to a FOIA request that it did not possess responsive records relating to specific FISA-authorized surveillance targets, hostile foreign powers could benefit from knowledge of this fact.

21. I am confident that the determination about the existence or nonexistence of the requested records being classified has not been made to conceal violations of law, inefficiency, or administrative error; to prevent embarrassment to a person, organization, or agency; to restrain competition; or to prevent or delay the release of information that does not require protection in the interests of national security. *See* Exec. Order No. 13526 § 1.7(a).

NSD's Exemption 6 Redactions

22. NSD also has redacted, and thus withheld, the names and contact information, including e-mail addresses and direct telephone numbers, of non-Senior Executive Service (SES) Executive Branch personnel engaged in their official duties. NSD FOIA withheld this information pursuant to FOIA Exemption 6 because the withheld portions of these records "would constitute a clearly unwarranted invasion of personal privacy of third parties." *See* 5 U.S.C. § 552(b)(6).

23. Though it is the general practice, NSD FOIA does not always redact such names. In this case, NSD balanced the privacy interests of the Executive Branch personnel identified in the documents, including their interests in avoiding publicity regarding aspects of their work,

against the public interest in the disclosure of this information. NSD has assessed that the legitimate public interest in the names and contact information of particular employees is minimal in this context because this information would not shed any meaningful light on NSD's or the Department's operations. As a result, NSD determined that the privacy rights of these individuals outweighed the public interest, if any, in the disclosure of the information. NSD determined, therefore, that releasing this information would constitute a clearly unwarranted invasion of these individuals' privacy which outweighs the public interest in disclosure.

Conclusion

I certify, pursuant to 28 U.S.C. § 1746, under penalty of perjury, that the foregoing is true and correct.

Executed this 2nd day of February, 2022, at Washington, D.C.

**PATRICK
FINDLAY**

Patrick N. Findlay

Digitally signed by PATRICK
FINDLAY
Date: 2022.02.02 10:40:47
-05'00'

Exhibit A

THE TRANSPARENCY PROJECT

P.O. Box 20753
Brooklyn, New York 11202
(979) 985-5289

October 26, 2018

Office of the Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, DC 20530-0001

Office of Legislative Affairs
U.S. Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, DC 20530-0001

National Security Division
U.S. Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, DC 20530-0001

Executive Office for U.S. Attorneys
U.S. Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, DC 20530-0001

Criminal Division
U.S. Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, DC 20530-0001

Federal Bureau of Investigation
935 Pennsylvania Avenue, NW
Washington, D.C. 20535-0001

Via electronic submission

To Whom It May Concern:

In 2017, the inspector general for the U.S. House of Representatives began investigating Imran Awan, Abid Awan, Jamal Awan, Hina Alvi, and Rao Abbas regarding mishandling of computer systems and electronic equipment. *See, e.g.*, Jenna Liffhits, “The IT guy and Wasserman Schultz,” June 15, 2018, *The Weekly Standard*, <https://www.weeklystandard.com/jenna-liffhits/the-strange-case-of-debbie-wasserman-schulzs-it-guy>. On behalf of The Transparency Project, and as permitted by the Freedom of Information Act, I request the following information from the respective entities to whom this letter is addressed:

1. Documents, files, records, and communications (regardless of electronic, paper or other format) referencing Imran Awan.
2. Documents, files, records, and communications (regardless of electronic, paper or other format) referencing Abid Awan.
3. Documents, files, records, and communications (regardless of electronic, paper or other format) referencing Jamal Awan.
4. Documents, files, records, and communications (regardless of electronic, paper or other format) referencing Hina Alvi.

5. Documents, files, records, and communications (regardless of electronic, paper or other format) referencing Rao Abbas.
6. From the National Security Division only, I request documents, files, records, and communications (regardless of electronic, paper or other format) referencing Seth Conrad Rich or "Seth Rich," who is deceased.

Each of the numbered items above should be considered a separate request.

The Transparency Project is a nonprofit Texas corporation and intends to use all of the information requested above to educate the public about government misconduct, therefore I request a waiver of any fees. If charges will apply, please let me know the approximate amount of such charges in advance. I can be reached by email at tyclevenger@yahoo.com if you need additional information.

Sincerely,

A handwritten signature in black ink, appearing to read 'Ty Clevenger', with a long horizontal flourish extending to the right.

Ty Clevenger
Executive Director
The Transparency Project

Exhibit B

THE TRANSPARENCY PROJECT

P.O. Box 20753
Brooklyn, New York 11202
(979) 985-5289

20-341 (Clevenger)

June 11, 2020

Office of the Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, DC 20530-0001

Office of Legislative Affairs
U.S. Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, DC 20530-0001

National Security Division
U.S. Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, DC 20530-0001

Executive Office for U.S. Attorneys
U.S. Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, DC 20530-0001

Criminal Division
U.S. Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, DC 20530-0001

Federal Bureau of Investigation
935 Pennsylvania Avenue, NW
Washington, D.C. 20535-0001

Via electronic submission

To Whom It May Concern:

On November 7, 2018, Judicial Watch, Inc. filed suit for information that sought pursuant to the Freedom of Information Act ("FOIA"), namely the following:

- (1) Any and all records related to any investigations or preliminary investigations involving former congressional IT support staffers Abid Awan, Imran Awan, Jamal A wan, and Hina R. Alvi. As part of this request, searches should of records [sic] should include, but not be limited to, the FBI automated indices, its older manual indices, and its Electronic Surveillance (EL SUR) Data Management System (EDMS), as well as cross-referenced files.
- (2) Any and all records of communication sent to or from FBI employees, officials or contractors involving the subjects in bullet item 1.

See Judicial Watch, Inc. v. U.S. Department of Justice, Case No. 1:18-cv-02563 (D.D.C.). As permitted by FOIA, and on behalf of the Transparency Project, I request the opportunity to view the same information, to include any information already provided to Judicial Watch.

The Transparency Project is a nonprofit Texas corporation and intends to use all of the information requested above to educate the public about government misconduct, therefore I request a waiver of any fees. If charges will apply, please let me know the

approximate amount of such charges in advance. I can be reached by email at tyclevenger@yahoo.com if you need additional information.

Sincerely,

A handwritten signature in black ink, appearing to read 'Ty Clevenger', with a long horizontal flourish extending to the right.

Ty Clevenger
Executive Director

Exhibit C

THE TRANSPARENCY PROJECT

P.O. Box 20753
Brooklyn, New York 11202
(979) 985-5289

June 15, 2020

FOIA Initiatives Coordinator
National Security Division
U.S. Department of Justice
950 Pennsylvania Avenue, N.W.
Room 6150
Washington, D.C. 20530-0001

20-333 (Clevenger)

Via email
nsdfoia@usdoj.gov

Federal Bureau of Investigation
Attn: FOI/PA Request
Record/Information Dissemination Section
170 Marcel Drive
Winchester, VA 22602-4843

Via facsimile
(540) 868-4997

To Whom It May Concern:

On or about November 23, 2019, an interview of Asst. Attorney General Bill Demers of the National Security Division was broadcast by CBS's *60 Minutes* news magazine. See "Trump DOJ official on 2016 Russian election hack: 'They were certainly looking to hurt Hillary Clinton.'" <https://www.cbsnews.com/news/trump-doj-official-on-2016-russian-election-hack-they-were-certainly-looking-to-hurt-hillary-clinton-60-minutes/>. In the interview with correspondent Bill Whitaker, Gen. Demers alleged that Russians hacked into Democratic National Committee servers in 2016 for the purpose of hurting presidential candidate Hillary Clinton.

During one clip of the interview, an announcer elaborated on the supporting evidence that the National Security Division claimed to have in its possession:

Assistant Attorney General John Demers runs the division, along with deputies Adam Hickey and Sean Newell. DOJ attorney, Heather Alpino, worked with special counsel Mueller on the Russian indictments. All have access to the underlying intelligence, and have no doubt the Russians interfered in the 2016 election.

The clip was followed by an exchange between Mr. Whitaker and Gen. Demers:

Bill Whitaker: This really happened.

John Demers: Yes. That really happened. And we believe that if we had to we could prove that in court tomorrow using only admissible, non-classified evidence to 12 jurors.

Bill Whitaker: Do you ever expect to get the 12 Russian officials to trial?

John Demers: I would be surprised. But the purpose of the indictment isn't just that, although that's certainly one of the purposes. The purpose of this kind of indictment is even to educate the public. For a legal document, the 29-page indictment is a page-turner. It details how U.S. intelligence agencies tracked each defendant's actions, sometimes by the keystroke, revealing the fictitious names and phony emails used to infiltrate the Democrats' computers, and tracing the stolen data on its circuitous route from Washington, D.C. to Moscow.

Bill Whitaker: The information in the indictment is very detailed. You have descriptions of the Russian agents typing into their computers.

John Demers: Obviously I can't go into too much detail because I don't wanna reveal investigative methods. But the insight here is that behind every one of those keyboards is not an IP address. It's a human being.

On behalf of The Transparency Project, and as permitted by the Freedom of Information Act, I request the opportunity to view the following:

- (a) All documents, records, communications, and other tangible evidence supporting Gen. Demers's claims to *60 minutes* above, *i.e.*, about Russian involvement in obtaining the DNC emails in 2016.
- (b) All documents, records, communications, and other tangible evidence relied on by Gen. Demers, Adam Hickey, Sean Newell, and Heather Alpino in support of their conclusions that Russians were responsible for obtaining the DNC emails in 2016.
- (c) All documents, records, communications, and other tangible evidence in the possession or control of the National Security Division concerning Seth Conrad Rich and/or Aaron Nathan Rich.
- (d) All documents, records, communications, and other tangible evidence in the possession or control of the National Security Division concerning other entities or individuals who may have played a role in stealing, hacking, leaking or improperly obtaining the DNC emails in 2016.
- (e) All documents, records, communications, and other tangible evidence in the possession or control of the National Security Division indicating whether the DNC emails were hacked externally, leaked from a source inside the DNC, or otherwise transmitted to third parties such as Wikileaks. If there was one or more than one instance of hacking, leaking, or other unauthorized transmission of DNC emails in 2016, please provide details for each such incident, *e.g.*, the dates,

persons and entities involved, the data that was hacked, leaked, or otherwise transmitted, and the means by which it was hacked, leaked, or transmitted.

- (f) All documents, records, communications, and other tangible evidence in the possession or control of the National Security Division or the FBI regarding whether Debbie Wasserman-Shultz or any other member of Congress was blackmailed or extorted, whether directly or indirectly, as a result of information procured by any of the following: Imran Awan, Abid Awan, Jamal Awan, Hina Alvi, Rao Abbas, or anyone affiliated with the government of Pakistan.

The Transparency Project is a nonprofit Texas corporation and intends to use all of the information requested above to educate the public about government misconduct, therefore I request a waiver of any fees. If charges will apply, please let me know the approximate amount of such charges in advance. I can be reached by email at tyclevenger@yahoo.com if you need additional information.

Sincerely,

A handwritten signature in black ink, appearing to read 'Ty Clevenger', with a long horizontal flourish extending to the right.

Ty Clevenger
Executive Director
The Transparency Project

Exhibit D

THE TRANSPARENCY PROJECT

P.O. Box 20753
Brooklyn, New York 11202
(979) 985-5289

20-338

June 18, 2020

Information and Privacy Coordinator
Central Intelligence Agency
Washington, D.C. 20505

Director, Information Management Division
Office of the Director of National Intelligence
Washington, D.C. 20511

FOIA Initiatives Coordinator
National Security Division
U.S. Department of Justice
950 Pennsylvania Avenue, N.W., Room 6150
Washington, D.C. 20530-0001

Federal Bureau of Investigation
Attn: FOI/PA Request
Record/Information Dissemination Section
170 Marcel Drive
Winchester, VA 22602-4843

Re: Freedom of Information Act Request

To Whom It May Concern:

I write on behalf of the The Transparency Project (“TTP”), a nonprofit corporation headquartered in Texas, to request information pursuant to the Freedom of Information Act, 5 U.S.C. § 552.

1. I request the opportunity to view all documents, records, communications and/or other tangible evidence reflecting or pertaining to surveillance of Edward Butowsky of Texas or Matt Couch of Arkansas. The term “surveillance” includes, but is not limited to, any attempt to hack into the computers, phones, other electronic devices, and/or online accounts of Mr. Butowsky or Mr. Couch. If any information obtained by surveillance was relayed to third parties, that information should be produced for inspection.
2. I request the opportunity to view all documents, records, communications and/or other tangible evidence pertaining to whether former Central Intelligence Agency Director David Petraeus mishandled classified information or sold such information during his tenure as CIA director. This request includes, but is not limited to, documents, records,

communications and/or other tangible evidence in the possession of the Office of the Inspector General of the CIA and/or the Office of the Intelligence Community Inspector General. This request further includes, but is not limited to, any draft indictments, draft arrest warrants, actual arrest warrants, and/or records of arrest.

I have attached release authorizations from Mr. Butowsky and Mr. Couch. TTP intends to use the requested information to educate the public about government misconduct, therefore I request a waiver of any fees. If charges will apply, please let me know the approximate amount of such charges in advance. I can be reached by email at tyclevenger@yahoo.com if you need additional information.

Sincerely,

A handwritten signature in black ink, appearing to read 'Ty Clevenger', with a long horizontal flourish extending to the right.

Ty Clevenger
Executive Director

Exhibit E

From: Mallory, Arnetta (NSD)
Sent: Wednesday, September 2, 2020 10:10 PM
To: tyclevenger@yahoo.com
Subject: NSD FOIA #20-341

Ty Clevenger
PO Box 20753
Brooklyn, NY 11202-0753

Re: FOIA/PA #20-341

Dear Mr. Clevenger:

This is to acknowledge your email dated June 11, 2020 to the Mail Referral Unit for information pertaining to (1) Any and all records related to any investigations or preliminary investigations involving former congressional IT support staffers Abid Awan, Imran Awan, Jamal Awan, and Hina R. Alvi. As part of this request, searches should of records [sic] should include, but not be limited to, the FBI automated indices, its older manual indices, and its Electronic Surveillance (EL SUR) Data Management System (EDMS), as well as cross-referenced files. (2) Any and all records of communication sent to or from FBI employees, officials or contractors involving the subjects in bullet item 1. Our FOIA office received your Freedom of Information Act request on June 19, 2020.

In response to the COVID-19 public health emergency, the NSD FOIA staff is teleworking full time. Our FOIA operations have been diminished while we are teleworking and our FOIA intake and FOIA processing will be slower than normal.

Please provide more clarity of your request to the National Security Division. Our Division does not maintain FBI records. If we do not receive a response from you within 30 days, your file will be administratively closed.

You may contact our Government Information Specialist, Arnetta Mallory, for any further assistance and to discuss any aspect of your request at:

U.S. Department of Justice
Records and FOIA Unit
3 Constitution Square
175 N Street N.E. 12th Floor
Washington, DC 20530
(202) 233-2639

Sincerely,

Arnetta Mallory
Government Information Specialist

Exhibit F



U.S. Department of Justice

National Security Division

Washington, D.C. 20530

Ty Clevenger
PO Box 20753
Brooklyn, NY 11202-0753

November 5, 2020

Re: FOIA/PA #20-333

Dear Mr. Clevenger:

This is to acknowledge your email dated June 15, 2020 attaching a Freedom of Information Act (FOIA) request. We received your Freedom of Information Act request on June 15, 2020 and have assigned it NSD #20-333.

Specifically, your request seeks:

(a) All documents, records, communications, and other tangible evidence supporting Gen. Demers's claims to 60 minutes above, i.e., about Russian involvement in obtaining the DNC emails in 2016.

(b) All documents, records, communications, and other tangible evidence relied on by Gen. Demers, Adam Hickey, Sean Newell, and Heather Alpino in support of their conclusions that Russians were responsible for obtaining the DNC emails in 2016.

(c) All documents, records, communications, and other tangible evidence in the possession or control of the National Security Division concerning Seth Conrad Rich and/or Aaron Nathan Rich.

(d) All documents, records, communications, and other tangible evidence in the possession or control of the National Security Division concerning other entities or individuals who may have played a role in stealing, hacking, leaking or improperly obtaining the DNC emails in 2016.

(e) All documents, records, communications, and other tangible evidence in the possession or control of the National Security Division indicating whether the DNC emails were hacked externally, leaked from a source inside the DNC, or otherwise transmitted to third parties such as Wikileaks. If there was one or more than one instance of hacking, leaking, or other unauthorized transmission of DNC emails in 2016, please provide details for each such incident, e.g., the dates, persons and entities involved, the data that was hacked, leaked, or otherwise transmitted, and the means by which it was hacked, leaked, or transmitted.

(f) All documents, records, communications, and other tangible evidence in the possession or control of the National Security Division or the FBI regarding whether Debbie Wasserman-Shultz or any other member of Congress was blackmailed or extorted, whether directly or indirectly, as a result of information procured by any of the following: Imran Awan, Abid Awan, Jamal Awan, Hina Alvi, Rao Abbas, or anyone affiliated with the government of Pakistan.

Three discrete categories of law enforcement and national security records are excluded from the

requirements of FOIA. *See* 5 U.S.C. § 552(c). This response is limited to those records that are subject to the requirements of FOIA. This is a standard notification that is given to all our requesters and should not be taken as an indication that excluded records do, or do not, exist. Additionally, NSD maintains investigative and prosecutorial files pertaining to subjects of NSD investigations. We do not routinely search these records in response to requests regarding NSD investigations in cases where the confirmation or denial of the existence of responsive records would, in and of itself, reveal information which would constitute a clearly unwarranted invasion of personal privacy of third parties or would reasonably be expected to interfere with enforcement proceedings. Accordingly, we can neither confirm nor deny the existence of records that may be potentially responsive to your request pursuant to 5 U.S.C. 552(b)(6) and/or (7)(A) and/or (7)(C).

Portions of your request are too broad in scope to identify any responsive records. Specifically, items (b), (d), and (f) are too broad for us to craft a search for records or to conclusively determine that we would neither confirm nor deny their existence without conducting a search. The Department of Justice regulations require that requests, must describe the records that you seek in enough detail to enable Department personnel to locate them with a reasonable amount of effort. And, whenever possible, your request should include specific information about each record sought, such as the date, title or name, author, recipient, and subject matter of the record.[28 CFR 16.3 (b)].

Please provide your response regarding items (b), (d), and (e) within 30 days of the date of this letter clarifying these items.

We will conduct searches for records in response to items (a), (c), and (f) that would not fall within the aforementioned scope of records whose existence the NSD can neither confirm nor deny.

As this matter is already in litigation, we are omitting our standard appeal paragraph. If you have any questions concerning this response please contact Assistant United States Attorney, Andrea Parker of the Eastern District of Texas at (409) 839-2538.

Notwithstanding the pending litigation, you may also contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire about the FOIA mediation services they offer to try to resolve disputes between FOIA requesters and federal agencies. The contact information for OGIS is as follows: Office of Government Information Services, National Archives and Records Administration, 8601 Adelphi Road-OGIS, College Park, Maryland 20740-6001, e-mail at ogis@nara.gov; telephone at (202) 741-5770; toll free at (877) 684-6448; or facsimile at (202) 741-5769. You also have the right to seek dispute resolution services through the DOJ's FOIA Public Liaison. NSD FOIA's Public Liaison, Patricia Matthews, may be reached by telephone at (202) 233-0756.

Sincerely,

ARNETTA
MALLORY

 Digitally signed by ARNETTA
MALLORY
Date: 2020.11.05 12:47:07 -05'00'

Arnetta Mallory
Government Information Specialist

Exhibit G



U.S. Department of Justice

National Security Division

Washington, D.C. 20530

Ty Clevenger
PO Box 20753
Brooklyn, NY 11202-0753
Via email: tyclevenger@yahoo.com

March 9, 2021

Re: FOIA/PA #20-333

Dear Mr. Clevenger:

This is our first interim response to your email dated June 15, 2020 attaching a Freedom of Information Act (FOIA) request.

Specifically, your request seeks:

(a) All documents, records, communications, and other tangible evidence supporting Gen. Demers's claims to 60 minutes above, i.e., about Russian involvement in obtaining the DNC emails in 2016.

(b) All documents, records, communications, and other tangible evidence relied on by Gen. Demers, Adam Hickey, Sean Newell, and Heather Alpino in support of their conclusions that Russians were responsible for obtaining the DNC emails in 2016.

(c) All documents, records, communications, and other tangible evidence in the possession or control of the National Security Division concerning Seth Conrad Rich and/or Aaron Nathan Rich.

(d) All documents, records, communications, and other tangible evidence in the possession or control of the National Security Division concerning other entities or individuals who may have played a role in stealing, hacking, leaking or improperly obtaining the DNC emails in 2016.

(e) All documents, records, communications, and other tangible evidence in the possession or control of the National Security Division indicating whether the DNC emails were hacked externally, leaked from a source inside the DNC, or otherwise transmitted to third parties such as Wikileaks. If there was one or more than one instance of hacking, leaking, or other unauthorized transmission of DNC emails in 2016, please provide details for each such incident, e.g., the dates, persons and entities involved, the data that was hacked, leaked, or otherwise transmitted, and the means by which it was hacked, leaked, or transmitted.

(f) All documents, records, communications, and other tangible evidence in the possession or control of the National Security Division or the FBI regarding whether Debbie Wasserman-Shultz or any other member of Congress was blackmailed or extorted, whether directly or indirectly, as a result of information procured by any of the following: Imran Awan, Abid Awan, Jamal Awan, Hina Alvi, Rao Abbas, or anyone affiliated with the government of Pakistan.

In an e-mail dated November 19, 2020, you indicated that "We would be willing to limit the initial search to Mr. Demers, but eventually we would like to see the relevant info for the other individuals."

We have conducted a search of the records of Mr. John Demers and located a record that is responsive to your request. We are withholding portions of that record pursuant to the following FOIA exemption set forth in 5 U.S.C. 552(b):

(6) Which permits the withholding of personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.

NSD is continuing to process remaining records that are responsive to your request. Please note that NSD is also conducting searches and processing records that are beyond the narrowed scope of just the records of Mr. Demers. We will provide you with an update, to include a possible supplemental production prior to the next (after the March 16, 2021) Joint Status Report in this matter.

Please note that three discrete categories of law enforcement and national security records are excluded from the requirements of FOIA. *See* 5 U.S.C. § 552(c). This response is limited to those records that are subject to the requirements of FOIA. This is a standard notification that is given to all our requesters and should not be taken as an indication that excluded records do, or do not, exist. Additionally, NSD maintains investigative and prosecutorial files pertaining to subjects of NSD investigations. We do not routinely search these records in response to requests regarding NSD investigations in cases where the confirmation or denial of the existence of responsive records would, in and of itself, reveal information which would constitute a clearly unwarranted invasion of personal privacy of third parties or would reasonably be expected to interfere with enforcement proceedings. Accordingly, we can neither confirm nor deny the existence of records that may be potentially responsive to your request pursuant to 5 U.S.C. 552(b)(6) and/or (7)(A) and/or (7)(C).

As this matter is already in litigation, we are omitting our standard appeal paragraph. If you have any questions concerning this response please contact Assistant United States Attorney, Andrea Parker of the Eastern District of Texas at (409) 839-2538.

Notwithstanding the pending litigation, you may also contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire about the FOIA mediation services they offer to try to resolve disputes between FOIA requesters and federal agencies. The contact information for OGIS is as follows: Office of Government Information Services, National Archives and Records Administration, 8601 Adelphi Road-OGIS, College Park, Maryland 20740-6001, e-mail at ogis@nara.gov; telephone at (202) 741-5770; toll free at (877) 684-6448; or facsimile at (202) 741-5769. You also have the right to seek dispute resolution services through the DOJ's FOIA Public Liaison. NSD FOIA's Public Liaison, Patricia Matthews, may be reached by telephone at (202) 233-0756.

Sincerely,

KEVIN TIERNAN
Digitally signed by KEVIN TIERNAN
Date: 2021.03.09 11:52:15 -05'00'
Kevin G. Tiernan
Records and FOIA

From: [Raimondi, Marc \(PAO\)](#)
To: [Demers, John C. \(NSD\)](#); [Andrews, Kelli \(NSD\)](#); [Hickey, Adam \(NSD\)](#); b6
Subject: 2019 10 31 GRU July 2018 Indictment Media Report
Date: Thursday, October 31, 2019 2:00:12 PM
Attachments: [2019 10 31 GRU July 2018 Indictment Media Report.docx](#)

John, when our intern b6 heard you were doing 60 Minutes on this case, she took it upon herself, unasked, to compile all the past clips for your review.

If you find it useful, please feel free to send her a note because I know she spent a good amount of time on it: b6

b6 /Adam, for your records. I messed with the margins a bit to get it down to 39 pages from 50.

GRU U.S. Election Hacking Indictment: July 13, 2018

Indictment

DOJ Press Release (full release is at the end of this document): [Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election](#)

Media Report Compiled on October 31st, 2019 for AAG Demers 60M Prep

Headlines:

[Mueller probe indicts 12 Russians with hacking of Democrats in 2016](#) *The Washington Post*

[12 Russian Agents Indicted in Mueller Investigation](#) *NYT*

[Justice Department Charges Russian Cyberspies With Attack On 2016 Election](#) *NPR*

[Russian intel officers charged with hacking Dems, Clinton to disrupt election](#) *NBC*

[12 Russians indicted in Mueller investigation](#) *CNN*

[Russian intelligence officers indicted in DNC hacking](#) *CBS*

[12 Russian intelligence officers indicted for hacking into DNC, Clinton campaign](#) *USA Today*

[Read Mueller's full indictment against 12 Russian officers for election interference](#) *PBS*

[Russian officers indicted for allegedly hacking Clinton campaign, DNC emails](#) *Fox News*

[Mueller indicts 12 Russians for DNC hacking as Trump-Putin summit looms](#) *POLITICO*

[Mueller Probe Indicts 12 Russians in Hacking of DNC and Clinton Campaign](#) *WSJ*

[U.S. accuses Russian spies of 2016 election hacking as summit looms](#) *Reuters*

[Russian Intelligence Officers Have Been Indicted For Hacking Hillary Clinton's Presidential Campaign](#) *BuzzFeed News*

[The Coincidence at the Heart of the Russia Hacking Scandal](#) *The Atlantic (Opinion)*

[Mueller's Politicized Indictment of Twelve Russian Intelligence Officers](#) *National Review (Opinion)*

The Washington Post July 13, 2018

A dozen Russian military intelligence officers were indicted Friday on charges they hacked Democrats' computers, stole their data and published those files to disrupt the 2016 election — the clearest connection to the Kremlin established so far by special counsel Robert S. Mueller III's investigation of interference in the presidential campaign.

The indictment against members of the Russian military agency known as the GRU marks the first time Mueller has taken direct aim at the Russian government, accusing specific military units and their named officers of a sophisticated, sustained effort to hack the computer networks of Democratic organizations and the Hillary Clinton campaign.

Deputy Attorney General Rod J. Rosenstein announced the charges at a midday news conference. Mueller, as has been his practice, did not attend the announcement. Court records show that a grand jury that Mueller has been using returned an indictment Friday morning.

The suspects "covertly monitored the computers, implanted hundreds of files containing malicious computer code, and stole emails and other documents," Rosenstein said. "The goal of the conspirators was to have an impact on the election. What impact they may have had . . . is a matter of speculation; that's not our responsibility."

The indictment comes days before President Trump is due to meet with Russian President Vladimir Putin in Finland. Rosenstein said he briefed Trump earlier this week on the charges.

Trump's lawyer Rudolph W. Giuliani said on Twitter that the indictments "are good news for all Americans. The Russians are nailed. No Americans are involved." He then called on Mueller "to end this pursuit of the president and say President Trump is completely innocent."

The 11-count, 29-page indictment describes in granular detail a carefully planned and executed attack on the information security of Democrats, as Russian government hackers implanted hundreds of malware files on Democrats' computer systems to steal information. The hackers then laundered the pilfered material through fake personas called DC Leaks and Guccifer 2.0, as well as others, to try to influence voters.

One of their conduits, identified in the indictment only as "Organization 1," was WikiLeaks, the global anti-secrecy group led by Julian Assange, according to people familiar with the case. The indictment describes WikiLeaks communicating with Guccifer 2.0 to obtain material.

On July 6, 2016, according to the indictment, WikiLeaks wrote, "if you have anything Hillary related we want it in the next twee [sic] days prefable [sic] because the DNC [Democratic National Convention] is approaching and she will solidify bernie supporters behind her after," referring to Clinton's rival for the Democratic nomination, Sen. Bernie Sanders (I-Vt.). WikiLeaks explained, "we think trump has only a 25% chance of winning against hillary . . . so conflict between bernie and hillary is interesting."

WikiLeaks released nearly 20,000 Democratic National Committee emails on the eve of the convention later that month, providing an embarrassing look at party operations and attitudes toward the Sanders campaign.

A former Justice Department official who was previously involved in the Russia probe said the charges should serve as a warning for the United States to buttress its election security as Americans prepare to vote in congressional elections in November.

"The detailed charges in this indictment make it unmistakably clear that the United States faces an aggressive, sophisticated adversary bent on using cyber means to subvert our democratic processes and institutions," said David Laufman, a former chief of the Justice Department's Counterintelligence and Export

The indictment offers troubling new accusations about the extent of Russian hacking efforts and interactions with Americans.

“On or about August 15, 2016, the conspirators, posing as Guccifer 2.0, received a request for stolen documents from a candidate for the U.S. Congress,” the indictment states. “The conspirators responded using the Guccifer 2.0 persona and sent the candidate stolen documents related to the candidate’s opponent.” The indictment does not identify the candidate.

The indictment also describes an online conversation between the GRU, posing as Guccifer 2.0, and a “person who was in regular contact with senior members of the presidential campaign of Donald J. Trump.”

People familiar with the case said that person is longtime Trump adviser Roger Stone. In August 2016, the hacker persona wrote: “please tell me if i can help u anyhow . . . it would be a great pleasure to me.”

Stone’s lawyer Grant Smith said, “It is clear from the indictment issued today that our client, Roger Stone, was not in any way involved with any of the alleged hacking of the 2016 election. As he testified before the House Intelligence Committee under oath, his 24-word exchange with someone on Twitter claiming to be Guccifer 2.0 is benign, based on its content, context and timing.”

U.S. officials identified one of the GRU sections that carried out the operations as Unit 26165, which worked out of a building about four miles from the Kremlin. It was responsible for hacking the DNC and the Democratic Congressional Campaign Committee, according to the indictment, which accuses Viktor Netyksho of being the military officer in command of Unit 26165 at the time.

Although the DNC was able to partially kick the Russian hackers out of its system in June 2016, the indictment says three months later, the GRU “successfully gained access to DNC computers hosted on a third-party cloud-computing service” which held “test applications related to the DNC’s analytics,” according to the indictment. The hacker stole that data from the DNC, the indictment said.

Another group of Russian military officers, Unit 74455, working out of a building that GRU officers referred to as the “Tower,” used fake online personas to spread stolen files, officials charged. The indictment identifies Col. Aleksandr Osadchuk as the commanding officer of that unit.

The indictment also notes an interesting development on July 27, 2016 — the day then-candidate Trump gave a press conference declaring his hope that missing Clinton emails would be found and made public, saying: “Russia, if you’re listening, I hope you’re able to find the 30,000 emails that are missing.”

The indictment says “on or about” that same day, “the conspirators attempted after hours to spearfish for the first time email accounts at a domain hosted by a third-party provider and used by Clinton’s personal office. At or around the same time, they also targeted seventy-six email addresses at the domain for the Clinton campaign.”

The Russian Foreign Ministry rejected the indictment’s allegations as lacking evidence and described the charges as a clear effort to derail the Trump-Putin summit in Helsinki.

“It is unfortunate that distributing false information has become the norm in Washington, and that criminal cases are being initiated based on clearly political motives,” the ministry said. Referring to the Mueller investigation, the statement went on: “The question remains how long this shameful comedy that is embarrassing the United States will go on.”

Rosenstein said the hackers interacted with some Americans in the course of their efforts but noted that those people had not been charged with a crime.

“When we confront foreign interference in American elections, it is important for us to avoid thinking politically as Republicans or Democrats and instead to think patriotically as Americans. Our response must not depend on who was victimized,” he said. “There will always be adversaries who work to exacerbate domestic differences and try to confuse, divide and conquer us. So long as we are united in our commitment to the values enshrined in the Constitution, they will not succeed.”

Mueller and a team of prosecutors [have been working since](#) May 2017 to determine whether any Trump associates conspired with Russia to interfere in the election. With the new indictment, his office has filed charges against 32 people on crimes including hacking, money laundering and lying to the FBI. Twenty-six of those charged are Russians who are unlikely to ever be put on trial in the United States.

In February, Mueller indicted a group of Russian Internet trolls who worked out of the Internet Research Agency, a company based in St. Petersburg and owned by a wealthy associate of Putin.

Trump’s former campaign manager, Paul Manafort, [is in jail in](#) Alexandria, Va., awaiting trial this month on financial fraud charges brought by Mueller but stemming from activities that predated the Trump campaign.

Mueller’s probe has come under sustained attack from Trump and at a press conference in England on Friday before Rosenstein spoke, the president again labeled the investigation a “witch hunt.”

“I think that we’re being hurt very badly by the — I would call it the witch hunt,” said Trump as he stood beside British Prime Minister Theresa May. “It really hurts our relationship with Russia.”

Rosenstein said of his decision to brief Trump, “It was important for the president to know what information we’ve uncovered because he’s got to make very important decisions for the country. He needs to understand what evidence we have of foreign election interference.”

[12 Russian Agents Indicted in Mueller Investigation](#)

NYT July 13, 2018

WASHINGTON — The special counsel investigating Russian interference in the 2016 election issued an indictment of 12 Russian intelligence officers on Friday in the hacking of the Democratic National Committee and the Clinton presidential campaign. The indictment came only three days before President Trump was planning to meet with President Vladimir V. Putin of Russia in Helsinki, Finland.

The 29-page indictment is the most detailed accusation by the American government to date of the Russian government’s interference in the 2016 election, and it includes a litany of brazen Russian subterfuge operations meant to foment chaos in the months before Election Day.

From phishing attacks to gain access to Democratic operatives, to money laundering, to attempts to break into state elections boards, the indictment details a vigorous and complex effort by Russia’s top military intelligence service to sabotage the campaign of Mr. Trump’s Democratic rival, Hillary Clinton.

The timing of the indictment, by Robert S. Mueller III, the special counsel, added a jolt of tension to the already freighted atmosphere surrounding Mr. Trump’s meeting with Mr. Putin. It is all but certain to feed into the conspiratorial views held by the president and some of his allies that Mr. Mueller’s prosecutors are determined to undermine Mr. Trump’s designs for a rapprochement with Russia.

The president has long expressed doubt that Russia was behind the 2016 attacks, and the 11-count indictment illustrates even more the distance between his skepticism and the nearly unanimous views of the intelligence and law enforcement agencies he leads.

“Free and fair elections are hard fought and contentious, and there will always be adversaries who work to exacerbate domestic differences and try to confuse, divide and conquer us,” Rod J. Rosenstein, the deputy attorney general, said Friday during a news conference announcing the indictment.

It was a striking statement a day after [Republican members of Congress, engaging in a shouting match during a hearing, attacked](#) Peter Strzok, the F.B.I. agent who oversaw the early days of the Russia investigation, and questioned the integrity of the Justice Department for what they charged was bias against the president.

The announcement created a bizarre split screen on cable networks of the news conference at the Justice Department and the solemn pageant at Windsor Castle in England, where Mr. Trump and his wife, Melania, were reviewing royal guards with Queen Elizabeth II.

Russia has denied that its government had any role in hacking the presidential election, and on Friday, Mr. Trump said he would confront Mr. Putin directly. But the president said he did not expect his Russian counterpart to acknowledge it.

“I don’t think you’ll have any, ‘Gee, I did it, you got me,’” Mr. Trump said during a news conference hours before the indictment was announced. He added that there would not be any “Perry Mason” — a reference to the 1950s and 1960s courtroom TV drama in which Perry Mason, a criminal defense lawyer played by Raymond Burr, often got people to confess. “I will absolutely firmly ask the question.”

But Mr. Trump also said he believed that the focus on Russia’s election meddling and whether his campaign was involved were merely partisan issues that made it more difficult for him to establish closer ties with Mr. Putin.

The Kremlin agreed. A statement on Friday from Russia’s Foreign Ministry said that the indictment was meant to “spoil the atmosphere before the Russian-American summit.”

After the indictment was announced, Senator Chuck Schumer of New York, the Democratic leader, and others in his party called on Mr. Trump to cancel his one-on-one meeting with Mr. Putin.

The indictment, Mr. Schumer said in a statement, was “further proof of what everyone but the president seems to understand: President Putin is an adversary who interfered in our elections to help President Trump win.” He added that “glad-handing with Vladimir Putin” would “be an insult to our democracy.”

The indictment builds on a declassified report released in January 2017 by several intelligence agencies, which concluded that “Putin and the Russian government aspired to help President-elect Trump’s election chances when possible by discrediting Secretary Clinton and publicly contrasting her unfavorably to him.”

Mr. Trump has long questioned the findings of intelligence agencies, suggesting alternate scenarios for who might have carried out the hacking campaigns. “It also could be somebody sitting on their bed that weighs 400 pounds, O.K.?” Mr. Trump said during the first presidential debate in September 2016.

Friday’s indictment did not include any accusations that the Russian efforts succeeded in influencing the election results, nor evidence that any of Mr. Trump’s advisers knowingly coordinated with the Russian campaign — a point immediately seized upon by the president’s allies.

Rudolph W. Giuliani, the president’s lawyer, said in a [Twitter post](#) that the indictment showed “no Americans are involved,” and he called on Mr. Mueller to end the inquiry. “The Russians are nailed,” Mr. Giuliani wrote.

Still, the indictment added curious new details to the events leading up to the November 2016 elections.

The indictment revealed that on July 27, 2016, Russian hackers tried for the first time to break into the servers of Mrs. Clinton’s personal offices. It was the same day that [Mr. Trump publicly encouraged Russia](#) to hack Mrs. Clinton’s emails.

“I will tell you this, Russia: If you’re listening, I hope you’re able to find the 30,000 emails that are missing,” Mr. Trump said during a news conference in Florida. “I think you will probably be rewarded mightily by our press.”

The indictment does not mention those remarks.

Separately, the indictment states that the hackers were communicating with “a person who was in regular contact with senior members of the presidential campaign.” Two government officials identified the person as Roger J. Stone Jr., a longtime adviser to Mr. Trump and the subject of close scrutiny by the F.B.I. and Mr. Mueller’s team. There is no indication that Mr. Stone knew he was communicating with Russians.

Communicating on Aug. 15 as Guccifer 2.0, an online persona, the Russian hackers wrote: “thank u for writing back ... do u find anyt[h]ING interesting In the docs i posted?”

Two days later, the hackers wrote the person again, adding, “please tell me If i can help u anyhow ... it would be a great pleasure to me.”

In another interaction several weeks later, the hackers, again writing as Guccifer 2.0, pointed to a document stolen from the Democratic Congressional Campaign Committee and posted online, asking, “what do u think of the info on the turnout model for the democrats entire presidential campaign.”

The person replied: “[p]retty standard.”

Friday’s indictment is a “big building block in the narrative being constructed for the American people regarding what happened during the election,” said Raj De, the chairman of the cybersecurity practice at Mayer Brown and the former general counsel of the National Security Agency.

By pulling together threads that Americans have read about for years — including the hacking of political institutions and campaigns, the dissemination of hacked emails and the attempts to compromise state election infrastructure — “this shows that the Russian campaign to impact the election was more coordinated and strategic than some have given it credit,” Mr. De said. “This indictment is our clearest window into that campaign.”

The document is a portrait of a coordinated and well-executed attack that targeted more than 300 people affiliated with the Clinton campaign, as well as other Democratic Party organizations. They implanted malicious computer code into computers, covertly monitored their users and stole their files that led to a series of disastrous leaks.

Investigators identified the 12 individuals in the indictment more than a year ago, according to a person with knowledge of the investigation who was not authorized to speak publicly about it.

Starting in April 2016, the hackers began to spread their stolen files using several online personas, including DC Leaks and Guccifer 2.0. The tens of thousands of stolen documents were released in stages that wreaked havoc on the Democratic Party throughout much of the election season.

The Russians also worked with people and organizations that were in a position to spread the information, including WikiLeaks, identified in the indictment as “Organization 1.”

According to the indictment, WikiLeaks wrote to Guccifer 2.0 in July 2016 asking for “anything Hillary related” in the coming days.

Most of the Russian intelligence officials charged in Friday’s indictment worked for the Russian military intelligence agency, formerly known as the G.R.U. and now called the Main Directorate.

While many of the broad elements of the Russian scheme were known before, investigators have not previously said how the Russian agents paid for the hacking campaign. The hackers’ use of cryptocurrency

The indictment released Friday said that the agents handled the most delicate transactions with the cryptocurrency [Bitcoin](#). The Malaysian computer server that hosted DCLeaks.com, for instance, was paid for with the virtual currency.

Because Bitcoin functions without any central authority, the technology “allowed the conspirators to avoid direct relations with traditional financial institutions, allowing them to evade greater scrutiny of their identities and sources of funds,” the indictment said.

The Russian agents had several methods for acquiring Bitcoin, according to the indictment. At one point, the agents were actually mining new Bitcoin, a process that involves using computers to unlock new Bitcoin by solving complex computational problems.

The indictment’s extraordinary details may raise pointed questions about actions taken and not taken by American intelligence agencies and the Obama administration as the Russian campaign unfolded.

In many instances, the indictment describes the actions of individual Russian intelligence officers on particular dates. It is unclear from the indictment whether American intelligence agencies, primarily the National Security Agency, were watching in real time as the Russians prepared for and carried out their attacks against Democratic targets in spring 2016.

It was not until October 2016 that the government put out its first public statement on the Russian intrusion. If Americans knew much earlier about Russian actions, there will be questions about why they did not warn the targets, try countermeasures or call Russia out publicly before they did.

It is possible, however, that American spies did not detect the Russian attacks in real time, but reconstructed them later by studying the hacked Democratic networks and possibly breaking into Russian systems to examine logs.

Some experts said that the granular detail in the indictment was a warning to groups who might be eyeing future attacks.

“Even from a historical perspective, I can’t think of a case when someone went into this level of naming and shaming,” said Thomas Rid, a professor of strategic studies at Johns Hopkins University. “This is really significant.”

“There is going to be a deterrent effect on third parties,” he said. “If you are doing this kind of work, there are now so many examples of you finding your name in an indictment, it will definitely have an effect.”

Justice Department Charges Russian Cyberspies With Attack On 2016 Election

NPR July 13th, 2018

The Justice Department charged 12 Russian intelligence officers on Friday with a litany of alleged offenses related to Russia's hacking of the Democratic National Committee's emails, state election systems and other targets in 2016.

Deputy Attorney General Rod Rosenstein, who announced the indictments, said the Russians involved belonged to the military intelligence service GRU. They are accused of a sustained cyberattack against Democratic Party targets, including its campaign committee and Hillary Clinton's campaign.

The GRU attackers also allegedly targeted state election systems, including government agencies and their vendors, and stole information about 500,000 American voters.

The attacks were a signature feature of [Russia's active measures](#) against the United States; embarrassing emails were passed to WikiLeaks, which released them publicly. The GRU also created other ways to pass the material it stole into the public, including a website called DCLeaks and a fake persona called "Guccifer 2.0."

The flood of embarrassing information about the inner workings of the Democratic Party's leadership led to the [resignation](#) of then-DNC Chairwoman Debbie Wasserman-Schultz. Later, Clinton's campaign chairman John Podesta also was embarrassed by the release of his emails.

The Russians named in the indictment discussed how and when to release material they had accumulated to make the biggest political splash inside the United States, Rosenstein said.

There is no allegation in the indictment that any American participated knowingly in the GRU cyberattacks, Rosenstein said.

Justice Department special counsel Robert Mueller is continuing to investigate whether anyone in the United States conspired with the Russian attack on the election.

But Rosenstein said that responsibility for this prosecution — which is unlikely to go forward to a trial in court as Russia is unlikely to extradite the suspects who have been charged — would pass from Mueller's office to the national security division of the Justice Department.

Friday's announcement follows [a separate but related indictment](#) by the special counsel's office from earlier this year of Russians allegedly connected to the campaign of social media agitation aimed at amplifying political controversy within the United States.

The Russian government has so far declined to extradite the people named, although one American attorney [has been arguing the case in Washington](#) on behalf of a company that's involved.

Cui bono?

Rosenstein asked Americans to not only focus on who was hurt by or benefited politically from the Russian attacks but to unite against foreign influence in the American democratic process.

"In my remarks, I have not identified the victims," Rosenstein said. "When we confront foreign interference in American elections, it is important for us to avoid thinking politically as Republicans or Democrats and instead to think patriotically as Americans. Our response must not depend on who was victimized."

The U.S. intelligence community has concluded, with further verification by the Senate intelligence committee, that Russia's active measures were aimed at hurting Clinton and helping Trump.

White House spokeswoman Lindsay Walter emphasized that no one in the Trump campaign was connected with the indictment unsealed on Friday.

"Today's charges include no allegations of knowing involvement by anyone on the campaign and no allegations that the alleged hacking affected the election result," she said. "This is consistent with what we have been saying all along."

Separately, one of Trump's lawyers, former New York Mayor Rudy Giuliani, welcomed the Justice Department announcement and said it showed that Mueller should finish up soon.

"The indictments Rod Rosenstein announced are good news for all Americans," [he wrote on Twitter](#). "The Russians are nailed. No Americans are involved. Time for Mueller to end this pursuit of the President and say President Trump is completely innocent."

The Americans who were unwittingly communicating with the Russian spies included a candidate for Congress — who is not identified — and at least one journalist. At least "one person who was in regular contact with senior members of the presidential campaign" also communicated with the GRU officers.

The indictment also says that on July 27, 2016, the GRU officers "attempted after hours to spearfish for the first time email accounts at a domain hosted by a third-party provider and used by Clinton's personal office." They also pinged 76 emails associated with the Clinton campaign.

July 27 was [the day that Trump said](#), "Russia, if you're listening, I hope you're able to find the 30,000 emails that are missing" from Clinton's email servers.

Geopolitical implications

Rosenstein's announcement took place just ahead of a planned meeting between President Trump and Russian President Vladimir Putin on Monday in Helsinki.

Trump told reporters Friday during his visit to the United Kingdom that he planned to "ask" Putin about Russia's attack on the election.

Trump has gone back and forth as to what he acknowledges about what took place and has cited Russia's official denials about its active measures. The president also has said the interference took place and vowed that if it returned in the 2018 midterm election — as U.S. intelligence officials have warned it may — he would "[counteract it very strongly](#)."

Rosenstein said the announcement of the charges on Friday took place because that was when the special counsel's office had completed its work investigating them and had the ability to present the evidence to a grand jury. The deputy attorney general said he had briefed the president about the matter.

Russia's foreign ministry said the indictments were an attempt to "spoil" the meeting.

Virginia Sen. Mark Warner, the top Democrat on the Senate intelligence committee, called on Trump to cancel his one-on-one meeting with Putin in Helsinki.

Warner told reporters on Capitol Hill that he worried that Trump's "ad hoc style" in which he "does not prepare" would be "taken advantage of" by Putin.

House Minority Leader Nancy Pelosi, D-Calif., said the indictment emphasized how tough Trump must be on Putin at their summit.

"The stakes for the upcoming Trump-Putin meeting could not be higher," Pelosi said. "President Trump must demand and secure a real, concrete and comprehensive agreement that the Russians will cease their ongoing attacks on our democracy. Failure to stand up to Putin would constitute a profound betrayal of the Constitution and our democracy."

Pelosi later joined other Democrats on Friday in calling for Trump to cancel his meeting with Putin.

Republicans stopped short of calling for Trump to cancel his meeting but some of them did also call for the president to take a firm line.

"All patriotic Americans should understand that Putin is not America's friend, and he is not the president's buddy," said Nebraska Sen. Ben Sasse. "We should stand united against Putin's past and planned future attacks against us."

South Carolina Rep. Trey Gowdy, chairman of the House oversight committee, echoed the note that Rosenstein sounded about how Americans of all political parties should be concerned about foreign election interference.

"I am pleased Russia is being held accountable for the actions against our country," Gowdy said. "This was not an attack on Republicans or an attack on Democrats — this was an attack on the United States."

The oversight committee plans to convene a hearing about election security by the end of July.

Russian intel officers charged with hacking Dems, Clinton to disrupt election

NBC July 13th, 2018

WASHINGTON — Twelve Russian intelligence officers have been indicted in connection with the bitcoin-funded hacking of Democratic organizations and the Hillary Clinton campaign "with the intent to interfere" in the 2016 election, officials announced Friday.

The charges, brought by special counsel Robert Mueller and announced by Deputy Attorney General Rod Rosenstein, come at a diplomatically sensitive time — just days before President Donald Trump meets formally for the first time with Russian President Vladimir Putin in Helsinki.

Among the new details: the conspirators allegedly first tried to compromise email accounts used by Clinton's personal office on July 27, 2016, the same day that Trump appeared to urge Russia to go after her emails at a campaign press conference in Florida.

Prosecutors say that in August 2016, a U.S. congressional candidate requested and received from stolen documents related to an opponent from an online persona created by the Russian cabal. And a state lobbyist received stolen data on Democratic donors later that month, the indictment alleges.

Rosenstein, who laid out the allegations at a news conference that began while Trump was meeting with Queen Elizabeth in London, said he had briefed Trump earlier in the week and that the president was "fully aware" of the charges in the indictment.

A statement from the White House did not address the allegations of Russian government interference and focused only on what was not in the indictment.

"Today's charges include no allegations of knowing involvement by anyone on the campaign and no allegations that the alleged hacking affected the election result. This is consistent with what we have been saying all along," the statement said.

The broad strokes of the hacking operation had already been made public, but the indictment provided new details and named names.

The court papers say that the defendants — two of whom were also charged with orchestrating attacks on state election systems — disseminated emails stolen from the Democrats through two online personas that they created, Guccifer 2.0 and DC Leaks.

William Bastone of the Smoking Gun website tweeted later Friday that he was the "U.S. reporter" referred to in the indictment who had received from Guccifer 2.0 the "password access to a nonpublic, password-protected website" that contained emails that had been stolen from "Victim 1."

The defendants used spear-phishing techniques to steal user names, passwords and emails and paid for the operation with bitcoin and other cryptocurrencies, the indictment alleges.

"The goal of the conspiracy was to have an impact on the election," Rosenstein said, adding that the indictment does not allege the Russian conduct changed the vote count or outcome of the 2016 election that put Trump in the White House.

Mueller, who has been investigating Russian interference in the 2016 election and possible collusion by the Trump campaign for more than a year, says the 12 defendants in Friday's indictment are members of the GRU, Russia's military intelligence agency.

Case 4:20-cv-00467-SDJ-CAN Document 69-2 Filed 09/27/22 Page 46 of 249 PageID #: 1888
Beginning in March 2016, they allegedly used fake identities and bogus accounts to trick volunteers and employees of Clinton's 2016 campaign and gain access to usernames and passwords that they used to steal emails and hack into other computers.

They allegedly also hacked into the networks of the Democratic Congressional Campaign Committee and the Democratic National Committee.

The goal of the conspiracy was to have an impact on the election.

The indictment says that in August and September 2016, Russians posing as Guccifer 2.0 were in contact with a person who communicated with senior Trump campaign officials, flagging emails posted and offering assistance.

"Please tell me if i can help u anyhow...it would be great pleasure to me," Guccifer 2.0 wrote, according to the indictment. The description matches a contact that longtime Trump associate Roger Stone has previously said he had with Guccifer.

The court papers also say that an unidentified organization — which matches the description of Wikileaks — coordinated the release of DNC emails with Guccifer 2.0 in July 2016 with an eye toward disrupting the party's convention.

"if you have anything hillary relayed we want it in the next tweo [sic] days prefable [sic] because the DNC is approaching and she will solidify bernie supporters behind her after," the organization wrote, according to the indictment.

DNC Chair Tom Perez said the latest indictments show the magnitude of the Russian operation. "This is not a witch hunt and it is certainly not a joke, as Donald Trump has desperately and incorrectly argued in the past," Perez said. "It's long past time for him and his allies in the Republican Party to stop ignoring this urgent threat to our national security."

The hackers were identified as Viktor Borisovich Netyksho, Boris Alekseyevich Antonov, Dmitriy Sergeyevich Badin, Ivan Sergeyevich Yermakov, Aleksey Viktorovich Lukashev, Sergey Aleksandrovich Morgachev, Nikolay Yuryevich Kozachek, Pavel Vyacheslavovich Yershov, Artem Andreyevich Malyshev, Aleksandr Vladimirovich Osadchuk, Aleksey Aleksandrovich Potemkin, and Anatoliy Sergeyevich Kovalev — all officials in Unit 26165 and Unit 74455 of GRU.

Kovalev is accused of targeting a state voter system in the U.S. In July 2016, he allegedly hacked the website of an unnamed state board of elections and stole information for 500,000 voters. The following month, he hacked into the computers of a U.S. vendor that supplied software used to verify voter registration information.

Friday's announcement isn't Mueller's first move against the Russians. In February, he brought charges against [13 Russian nationals](#) who allegedly carried out a campaign of social media-fueled [information warfare](#) — some of it supporting Trump and disparaging Clinton — that he said was aimed at meddling in the 2016 election.

[12 Russians indicted in Mueller investigation](#)

CNN July 14th, 2018

Washington (CNN)The Justice Department announced [indictments against 12 Russian nationals](#) as part of special counsel Robert Mueller's investigation of Russian interference in the 2016 election, accusing them of engaging in a "sustained effort" to hack Democrats' emails and computer networks.

All 12 defendants are members of the GRU, a Russian federation intelligence agency within the main intelligence directorate of the Russian military, who were acting in "their official capacities."

The revelations provide more detail on the sophisticated assault on the US election in 2016, including the release of emails designed to damage Democratic presidential candidate Hillary Clinton.

The indictment was announced at almost exactly the moment that President Donald Trump rolled into the quadrangle of [Windsor Castle to meet the awaiting Queen Elizabeth II](#) in the symbolic highpoint of his visit to Britain.

Trump is due to meet Russian President Vladimir Putin -- who has denied election meddling -- in Helsinki on Monday for a summit that includes a one-on-one meeting with only interpreters present. White House press secretary Sarah Sanders said Friday the summit will not be canceled.

The Justice Department says the hacking targeted Clinton's campaign, Democratic National Committee and the Democratic Congressional Campaign Committee, with the intention to "release that information on the internet under the names DCLeaks and Guccifer 2.0 and through another entity."

Deputy Attorney General Rod Rosenstein said the indictment does not name any American citizen, but told reporters that defendants "corresponded with several Americans during the course of the conspiracy through the internet."

"There is no allegation in this indictment that any American citizen committed a crime," Rosenstein said at a news conference. "There is no allegation that the conspiracy altered the vote count or changed any election result."

Deputy White House press secretary Lindsay Walters referenced Rosenstein's comments and said there is no evidence tying the Trump campaign to hacking attempts.

"Today's charges include no allegations of knowing involvement by anyone on the campaign and no allegations that the alleged hacking affected the election result," Walters said in a statement. "This is consistent with what we have been saying all along."

Trump private attorney Rudy Giuliani [in a tweet](#) said the indictments are "good news for all Americans" but called on the special counsel investigation to end.

"The Russians are nailed. No Americans are involved. Time for Mueller to end this pursuit of the President and say President Trump is completely innocent," he tweeted.

Trump, meanwhile, did not criticize Putin or condemn Russia's actions in a pair of tweets on Saturday, instead attacking his predecessor, former President Barack Obama, with what has become a [familiar claim](#) of his.

"The stories you heard about the 12 Russians yesterday took place during the Obama Administration, not the Trump Administration," [Trump wrote](#). "Why didn't they do something about it, especially when it was reported that President Obama was informed by the FBI in September, before the Election?"

"These Russian individuals did their work during the Obama years," [Trump continued in a tweet later Saturday](#). "Why didn't Obama do something about it? Because he thought Crooked Hillary Clinton would win, that's why. Had nothing to do with the Trump Administration, but Fake News doesn't want to report the truth, as usual!"

Obama, however, personally warned Putin against messing with the election, imposed sanctions on Russian individuals and entities, kicked out 35 Russian diplomats and closed two of the Kremlin's compounds in the United States.

Announced as Trump meets Queen Elizabeth II

Asked about the timing of the announcement, Rosenstein said it came as "a function of the collection of the facts, the evidence, the law, and a determination that it was sufficient to present the indictment at this time."

The unfolding drama on both sides of the Atlantic reflected how Trump's presidency has been overshadowed by the Mueller probe from its earliest moments and how the investigation frequently tramples the President's attempts to carve out favorable headlines.

Some lawmakers are calling on Trump to cancel the meeting with Putin.

"Glad-handing with Vladimir Putin on the heels of these indictments would be an insult to our democracy," [said Senate Minority Leader Chuck Schumer](#).

"President Trump must be willing to confront Putin from a position of strength and demonstrate that there will be a serious price to pay for his ongoing aggression towards the United States and democracies around the world," said GOP Sen. John McCain in a statement. "If President Trump is not prepared to hold Putin accountable, the summit in Helsinki should not move forward."

In a statement, Russia's foreign ministry said there was no basis for the charges and said purpose of the announcement is to "spoil the atmosphere" before Monday's summit.

"It is regrettable that the duplication of false information in Washington has become the norm, and criminal cases are worked up for obvious political reasons. The question remains: how long will they continue to break this shameful comedy that disgraces the US," the Russian statement said.

Russian military stole information of 500,000 voters

Eleven of the Russians are charged with identity theft, conspiracy to launder money and conspiracy to commit computer crimes. Two defendants are charged with a conspiracy to commit computer crimes.

"Russian GRU officers hacked the website of a state election board and stole information about 500,000 voters," Rosenstein said. "They also hacked into computers of a company that supplied software used to verify voter registration information."

The defendants worked for two units of the GRU that "engaged in active cyber operations to interfere in the 2016 presidential elections," Rosenstein said. One unit stole information using spearfishing schemes and hacked into computer networks where they "installed malicious software that allowed them to spy on users and capture keystrokes, take screenshots and exfiltrate or remove data from those computers."

Intelligence gathered by US officials captured some of the Russians accused in Friday's indictments congratulating each other and celebrating the success of their operation during the campaign, according to a person familiar with the investigation. They were also captured celebrating Trump's victory. The source said the intelligence was gathered both before and after the 2016 election.

Each of the Russians involved held military titles. One leader was Sergey Aleksandrovich Morgachev, a lieutenant colonel who used the hacking tool "X-Agent." The other Russians involved also used various pseudonyms to send phishing emails to Democratic Party affiliates.

The two-part operation started with a "spearfishing" effort in early 2016, the indictment describes. The Russians hit more than 300 people connected to the Clinton campaign and Democratic political groups.

One of those targets was Clinton campaign chairman John Podesta, whom Aleksey Viktorovich Lukashev and others spammed with a link that appeared to come from Google as a security notification but led Podesta

The computer crimes the Russians face also accuse them of installing malware on Democratic campaign computers. That allowed them to steal passwords, record staffers' keystrokes, take screenshots and observe computer work done on fundraising and voter outreach projects, according to the indictments. They also watched a Democratic campaign committee employee access the organization's bank account information.

Though the Democratic organizations realized they were hacked by May 2016 and attempted to flush out the hackers, the Russians continued to watch the computers through their hacks until a month before the election, according to the indictment.

They then worked to distribute the documents starting in June 2016. The Russian intelligence agents had registered the website DCLeaks.com and started a Facebook page and Twitter feed claiming they were "American hacktivists." Once the DNC announced publicly it had been hacked, the Russians used the online moniker Guccifer 2.0, claiming they were a lone Romanian. They did this "to undermine the allegations of Russian responsibility for the intrusion," the indictment said. They also took steps to cover their tracks, deleting files and logs on computers.

In June 2016, Guccifer 2.0 began posting stolen documents through a Wordpress site they ran. To spread the material further, they shared stolen documents with people including a US congressional candidate, a state lobbyist, journalists, an entity known as Organization 1, which appears to be Wikileaks, and a person in touch with the Trump campaign.

It has been more than a year since the special counsel's Russia investigation began. The probe had already resulted in criminal charges against 14 Russians, five Americans and one Dutch citizen and three corporate entities. One of those people has already been sentenced and served a month in prison, while three others pleaded guilty and await sentencing.

A number of Trump associates have so far been swept up in the special counsel investigation.

Paul Manafort, Trump's campaign chairman in 2016, is currently in jail after his bail was revoked for alleged witness tampering and faces two sets of criminal charges related to his years of working as a lobbyist for pro-Russian Ukrainian politicians. He has maintained his innocence and is set to go to trial on bank fraud and other financial allegations on July 25.

Former Trump campaign official and Manafort deputy Rick Gates, former Trump campaign aide George Papadopoulos and former Trump White House national security adviser Michael Flynn have all entered guilty pleas in connection with the investigation. Gates, Papadopoulos and Flynn have all pleaded guilty to making false statements to investigators. All agreed to cooperate with the special counsel's office, but Papadopoulos' cooperation is likely to come to an end in September when he is sentenced. The four Trump associates that have been charged are not accused of helping Russia meddle in the election.

Russian intelligence officers indicted in DNC hacking

CBS July 13, 2018

Twelve Russians have been indicted by a grand jury in the special counsel probe for alleged hacking during the 2016 election, including for hacking emails of the Democratic National Committee, Deputy Attorney General Rod Rosenstein announced Friday.

Rosenstein said the 12 defendants are all members of the Russian intelligence arm GRU, and attempted to interfere with the 2016 presidential election by "spear phishing" volunteers and employees of Hillary Clinton's campaign. By allegedly doing this — tricking staffers into clicking on emails from rogue accounts — they were able to steal usernames and passwords, eventually hacking into the networks of the Democratic

Case 4:20-cv-00467-SDJ-CAN Document 69-2 Filed 09/27/22 Page 50 of 249 PageID #: 1892
National Campaign Committee and Democratic National Committee. The GRU, Rosenstein said, created and controlled the groups D.C. Leaks and Guccifer 2.0., which in 2016, posted thousands of emails from Democratic party officials.

"The object of the conspiracy was to hack into the computers of U.S. persons and entities involved in the 2016 presidential election, steal documents from those computers, and stage releases of the stolen documents to interfere with the 2016 U.S. presidential election," the indictment reads.

The indictment says that the alleged conspirators "spearphished individuals affiliated with the Clinton campaign throughout the summer of 2016," and then goes on to say that "on or about July 27, 2016, the conspirators attempted after hours to spearfish for the first time email accounts at a domain hosted by a third-party provider and used by Clinton's personal office. At or around the same time, they also targeted seventy-six email addresses at the domain for the Clinton campaign."

Also on July 27, 2016, when those efforts had already been ongoing, Donald Trump expressed the hope that Russia would find Clinton's missing emails. "I will tell you this -- Russia, if you're listening, I hope you're able to find the 30,000 emails that are missing. I think you will probably be rewarded mightily by our press," the GOP presidential nominee said at a press conference in Miami.

The indictment also claims in a related allegation that Russian officers hacked a state election board's website and stole the information of roughly 500,000 voters. The indictment also alleges the GRU officers hacked into computers belonging to a company that supplies software used to verify voter information, and targeted local and state election offices.

Rosenstein made it clear that no Americans are accused of any wrongdoing in this indictment.

"There is no allegation in this indictment that Americans knew they were corresponding with Russian intelligence officers," said Rosenstein, who also noted there is no evidence the alleged hacking had any impact on the election results.

The indictment does mention that Russians provided opposition research to a congressional candidate, although that individual is not named.

The indictment claims the conspirators, posing as Guccifer 2.0, "received a request for stolen documents from a candidate for the U.S. Congress. The Conspirators responded using the Guccifer 2.0 persona and sent the candidate stolen documents related to the candidate's opponent," the indictment reads.

The charges come just days before President Trump is set to meet with Russian President Vladimir Putin in Helsinki, Finland. Sen. Mark Warner, the vice chairman of the Senate Intelligence Committee, said Mr. Trump shouldn't be meeting with Putin one-on-one.

"There should be no one-on-one meeting between this president and Mr. Putin. There needs to be other Americans in the room," Warner told reporters Friday.

Rosenstein said he briefed Mr. Trump on the indictment earlier this week.

"I'll allow president to speak for himself," Rosenstein said when asked for Mr. Trump's response to the news. "Obviously it's important for the president to know what information we've uncovered because he's got to make very important decisions for the country. So he needs to understand what evidence we have of foreign election interference."

Hours before the DOJ announcement, in a press conference with British Prime Minister Theresa May, Mr. Trump called the Russia investigation into election meddling and any ties to Trump associates a "rigged witch hunt."

"Today's charges include no allegations of knowing involvement by anyone on the campaign and no allegations that the alleged hacking affected the election result. This is consistent with what we have been saying all along," White House Deputy Press Secretary Lindsay Walters said.

Back in July 2016, Mr. Trump tweeted that the "new joke in town" is Russia leaked the "disastrous DNC emails."

"The new joke in town is that Russia leaked the disastrous DNC e-mails, which should never have been written (stupid), because Putin likes me," he tweeted on July 25, 2016.

Rudy Giuliani, the lawyer who is aiding Mr. Trump in the Russia investigation, used Rosenstein's announcement as an opportunity to call on Mueller to end his investigation and declare Mr. Trump's innocence.

When a reporter in London asked Mr. Trump if he would bring up election meddling with Putin, Mr. Trump said he would.

The charges come after Mueller's investigation has already led to the [indictment of 13 Russian nationals](#) who were accused of manipulating social media.

In the face of alleged foreign interference, Rosenstein urged unity and patriotism against foreign interference.

"When we confront foreign interference in American elections, it is important for us to avoid thinking politically as Republicans or Democrats and instead to think patriotically as Americans. Our response must not depend on who was victimized," Rosenstein said in his prepared remarks.

"The blame for election interference belongs to the criminals who committed election interference," the deputy attorney general added. "We need to work together to hold the perpetrators accountable, and keep moving forward to preserve our values, protect against future interference, and defend America."

It is unclear, if not unlikely, however, that the indicted Russians will ever see a courtroom. The U.S. does not have an extradition treaty with Russia.

12 Russian intelligence officers indicted for hacking into DNC, Clinton campaign

USA Today July 13th, 2018

WASHINGTON — Twelve Russian military intelligence officers were charged Friday in a far-reaching hacking scheme that targeted the Democratic National Committee and the Clinton presidential campaign as part of the Kremlin's effort to undermine the 2016 election, the Justice Department announced.

The 11-count indictment, unveiled [just days before](#) President Donald Trump was set to meet with Russian President Vladimir Putin in Helsinki, Finland, asserts that the Russian suspects "engaged in a sustained effort" to penetrate the most sensitive repositories of information held by the Democratic Party.

Deputy Attorney General Rod Rosenstein announced the action, part of the continuing investigation into Russia's interference in the 2016 campaign by special counsel Robert Mueller, as some Democratic lawmakers called on the White House to immediately punish the Kremlin by canceling the Putin meeting.

The White House did not immediately address that demand Friday, but rather reasserted that the indictment had not implicated anyone connected to the campaign.

"Today's charges include no allegations of knowing involvement by anyone on the campaign and no allegations that the alleged hacking affected the election result," White House spokeswoman Lindsay Walters said. "This is consistent with what we have been saying all along."

While Friday's announcement came as [Trump was meeting with Queen Elizabeth II](#) during his trip to the United Kingdom, Rosenstein said that he had briefed Trump earlier this week before his departure abroad.

At the heart of the case, Mueller's team charged that the Russian operatives sought to "steal documents" from the Democrat computer systems and "stage the release... to interfere with the 2016 U.S. presidential election."

The charges build on a case Mueller brought in February, charging 13 Russian nationals and three businesses – including an internet firm tied to the Kremlin – with waging "information warfare against the United States" with the goal of "spreading distrust toward the candidates and the political system."

Still, Friday's indictment contained no allegations that the actions altered the vote count or changed the outcome of the 2016 presidential elections.

"Free and fair elections are hard-fought and contentious, and there will always be adversaries who work to exacerbate domestic differences and try to confuse, divide and conquer us," Rosenstein said. "So long as we are united in our commitment to the shared values enshrined in the Constitution, they will not succeed."

Among the jarring disclosures in the 29-page indictment included the allegation that the Russian intelligence officials first sought to penetrate email accounts associated with Clinton's personal offices on July 27, 2016.

Earlier that same day, then-candidate Trump appeared to enlist Russia in a similar effort.

"Russia, If you're listening, I hope you're able to find the 30,000 emails that are missing," Trump said at the time, referring to Clinton's use of a private email server while she was secretary of State.

Also contained in Friday's court documents, federal prosecutors said that the Russian operatives in August 2016 "received a request for stolen documents [from a candidate for U.S. Congress](#)."

According to court papers, the suspects posing as online activists later sent the unnamed candidate stolen information related to the candidate's opponent.

The group also allegedly conspired to hack into computers of state election boards, secretaries of State and U.S. companies that supplied software and other technology related to election administrations. According to court papers, the personal information of at least 500,000 voters was stolen from one state election organization.

Because the Russian officials remain in Russia, it is highly unlikely that they will ever be prosecuted in the United States. Nevertheless, the U.S. action follows a practice of so-called "naming and shaming" of foreign government operatives implicated in actions against the U.S.

The indictment included charges of conspiracy, aggravated identity theft and money laundering. Federal prosecutors asserted that the Russian hackers corresponded with "several" Americans. But Rosenstein said there was no evidence that the Americans were aware that they were corresponding with Russian intelligence officers.

The deputy attorney general said the announcement of the charges were made with "no regard to politics," adding that the evidence was "sufficient" to bring the case.

The suspects, according to the indictment, were attached to two military divisions of Russia's Main Intelligence Directorate, known as the GRU — Unit 26165 and Unit 74455. In 2016, Unit 26165 operatives

Case 4:20-cv-00467-SDJ-CAN Document 69-2 Filed 09/27/22 Page 53 of 249 PageID #: 1895
allegedly launched spearphishing campaigns — sending misleading emails to targets in attempts to steal usernames, passwords and other personal information — against the Clinton campaign.

Those stolen credentials, according to federal prosecutors, were used to hack into the DCCC and the DNC. At the same time, the suspects were able to "monitor" the activities of dozens of staffers and "implant hundreds of malicious files to steal passwords and maintain access to these networks."

Democratic National Committee Chairman Tom Perez said that while the DNC was a primary target of the attack, the indictment outlines a vast disruption effort.

"Donald Trump has desperately been calling this investigation a witch hunt. But once again we have cold hard proof that he is absolutely wrong," Perez said. "This is not a witch hunt. This is not a joke. This is an attack on our democracy."

Democratic lawmakers described the charges as only further proof of what the U.S. intelligence community determined long ago: that Russia sought to tilt the election to Trump's favor.

"President Putin is an adversary who interfered in our elections to help President Trump win," Senate Minority Leader Chuck Schumer, D-N.Y., said. "President Trump should cancel his meeting with Vladimir Putin until Russia takes demonstrable and transparent steps to prove that they won't interfere in future elections. Glad-handing with Vladimir Putin on the heels of these indictments would be an insult to our democracy."

Schumer was joined in the call by a coalition of Democrat lawmakers, including Virginia Sen. Mark Warner, the senior Democrat on the Senate Intelligence Committee.

House Democratic Leader Nancy Pelosi said the indictment highlighted "a massive, concerted operation to interfere in our elections," and she warned that the Kremlin "will do so again in the fall."

"Strong, immediate action is needed to secure our state election systems," Pelosi said.

She continued: "The stakes for the upcoming Trump-Putin meeting could not be higher. President Trump must demand and secure a real, concrete and comprehensive agreement that the Russians will cease their ongoing attacks on our democracy. Failure to stand up to Putin would constitute a profound betrayal of the Constitution and our democracy."

Arizona Sen. John McCain, the Republican chairman of the Armed Services Committee, also urged Trump to use Friday's indictment to confront the Russian leader.

"If President Trump is not prepared to hold Putin accountable, the summit in Helsinki should not move forward," McCain said.

Republican House Foreign Affairs Committee Chairman Ed Royce of California, meanwhile, argued that the charges demonstrate that the Trump administration was holding Russia "accountable."

"For years, we've known about the Kremlin's campaign to weaponize information and chip away at our institutions," Royce said. "And yet for years, we have not done enough to counter it. I'm glad that's begun to change, thanks in part to Congress, but there's much more to be done."

Sen. Ben Sasse, R-Neb., said the criminal charges should serve to unite Americans to push back against the Kremlin's disruption campaign.

"This is not a Republican or a Democrat view -- it is simply the reality," Sasse said. "All patriotic Americans should understand that Putin is not America's friend, and he is not the president's buddy."

[Read Mueller's full indictment against 12 Russian officers for election interference](#)

Twelve Russian intelligence officers were accused Friday of trying to interfere in the 2016 presidential elections, including a hack of Democratic National Committee.

The allegations came in the latest indictment from special counsel Robert Mueller's investigation into Russian interference in the elections and possible ties to President Donald Trump's campaign. The announcement comes days before Trump's scheduled meeting with Russian President Vladimir Putin; the president pledged this morning during his visit with British Prime Minister Theresa May to raise the issue of election meddling with Putin.

According to the indictment, the officers worked for a military agency known as "GRU," which conspired to hack into computers of those working on the elections with the goal of stealing and releasing documents. That includes the DNC, but also computers associated with the Democratic Congressional Campaign Committee as well as those of volunteers and employees of the Hillary Clinton campaign.

Starting in June 2016, they released tens of thousands of these documents using online pseudonyms, such as "Guccifer 2.0" and "DC Leaks." They used a network of computers around the world, a system paid for with cryptocurrency, to conceal their identities.

They also broke into the computers of those charged with overseeing elections, including state election officials and secretaries of state, as well as companies in charge of election technology and software.

Deputy Attorney General Rod Rosenstein said he has no evidence that the hacking changed the outcome of the 2016 election, nor that "any American was a knowing participant in the alleged unlawful activity."

Russian officers indicted for allegedly hacking Clinton campaign, DNC emails

Fox News July 13th, 2018

A federal grand jury has indicted 12 Russian intelligence officers for allegedly hacking emails from the Hillary Clinton campaign and Democratic Party during the 2016 election, the Justice Department announced Friday.

"The internet allows foreign adversaries to attack America in new and unexpected ways," Deputy Attorney General Rod Rosenstein said during a press conference.

All 12 defendants are members of GRU, the Russian intelligence agency.

The case stems from Special Counsel Robert Mueller's probe into Russia's efforts to interfere in the 2016 presidential election. It comes as President Trump plans to meet Russian President Vladimir Putin for a summit in Helsinki on Monday.

The indictment amounted to the clearest allegation yet of Russian meddling in the election, blaming Moscow for the email hacking scandal that rocked the 2016 race by revealing embarrassing and politically damaging discussions by major Democrats. The charges swiftly fueled calls from Democratic lawmakers for Trump to cancel his Putin summit.

But as Trump continues to describe the probe as a "witch hunt," the White House downplayed the allegations.

"Today's charges include no allegations of knowing involvement by anyone on the campaign and no allegations that the alleged hacking affected the election result," said Lindsay Walters, the deputy White House press secretary. "This is consistent with what we have been saying all along."

Case 4:20-cv-00467-SDJ-CAN Document 69-2 Filed 09/27/22 Page 55 of 249 PageID #: 1897
Of the 12 defendants, 11 are charged with conspiracy to commit computer crimes, eight counts of aggravated identity theft and conspiracy to launder money. Another is charged with a separate conspiracy to commit computer crimes.

The 29-page indictment says starting in March 2016, the Russian agents used “a variety of means to hack the email accounts of volunteers and employees” of Hillary Clinton’s campaign. Her campaign chairman, John Podesta, famously had his emails leaked during the campaign.

They also targeted campaign committees, like the Democratic National Committee and the Democratic Congressional Campaign Committee, the indictment said.

“The conspirators covertly monitored the computers of dozens of DCCC and DNC employees, implanted hundreds of files containing malicious computer code and stole emails and other documents from the DCCC and DNC,” it read.

By April 2016, according to the documents, the defendants began to release the hacked materials to the public by using fictitious online personas like DCLeaks and Guccifer 2.0.

The indictment comes as Mueller's team has investigated whether anyone associated with the Trump campaign assisted the Russians.

But during his press conference, Rosenstein said, "there is no allegation in this indictment that any American citizen committed a crime."

He also said, "There is no allegation that the conspiracy changed the vote count or affected any election result. The special counsel's investigation is ongoing."

Director of National Intelligence Dan Coats, reacting to the indictment and the broader cyber threat on Friday, said there is “not yet” this kind of electoral interference happening in the midterms – but warned history could repeat itself.

“In regards to state actions, Russia has been the most aggressive foreign actor. No question,” he said. “We are not yet seeing the kind of electoral interference in specific states and voter databases that we experienced in 2016. However, we fully realize that we are just one click away ... from a similar situation repeating itself.”

Oleksandr Danylyuk, a military and intelligence expert on Russian information operations, told Fox News he believes Russia “does not stop its active measures in the inter-election period.”

“Politicians of both camps should understand that the United States is under a hybrid attack,” said Danylyuk, who chairs the Center for Defense Reforms in Ukraine. “In this regard, they have to put state interests above their party interests.”

He also called on journalists to be aware of how they can be used.

“Much of the kompromat will be provided by Russian proxies directly to American politicians and journalists,” Danylyuk said. “They must fight the temptations to use this information without checking its reality.”

The Rosenstein announcement came at the same time Trump was meeting with Queen Elizabeth II in England, with plans to meet Putin for a summit on Monday. Trump has previously cited Putin's denials of election interference, while saying he would like their two countries to get along.

“President Trump should cancel his meeting with Vladimir Putin until Russia takes demonstrable and transparent steps to prove that they won’t interfere in future elections,” Senate Minority Leader Chuck

Rosenstein said he briefed the president on the charges this week.

Though the indictment listed the Democratic groups, Rosenstein made a point of not naming the political affiliation of the hacked organizations during his press statement, saying it's important to think "patriotically" and not politically in the face of such threats.

Florida Rep. Debbie Wasserman Schultz, who served as chairman of the Democratic National Committee during the time period, took aim at Trump in a statement.

"I'm pleased that the Justice Department is following the facts wherever they may lead, despite Donald Trump's dangerous distortions and his refusal to acknowledge the conclusions reached by the American intelligence community," she said.

Russian individuals have [previously](#) been indicted as part of the case. In February, Mueller brought a case against 13 Russians and three Russian companies who are accused of setting a "strategic goal to sow discord in the U.S. political system, including the 2016 presidential election."

In that case, the defendants are accused of spreading derogatory information about Clinton, denigrating Republican candidates Ted Cruz and Marco Rubio -- and ultimately supporting Democratic candidate Bernie Sanders and then-Republican candidate Donald Trump.

[Mueller indicts 12 Russians for DNC hacking as Trump-Putin summit looms](#)

POLITICO July 13th, 2018

Special counsel Robert Mueller indicted 12 Russian military officials on Friday and accused them of hacking into two Democratic Party computer systems to sabotage the 2016 presidential election.

Deputy Attorney General Rod Rosenstein announced the indictment, filed in federal district court in Washington, just days before a scheduled Monday summit in Helsinki between President Donald Trump and Russian President Vladimir Putin. U.S. intelligence agencies have assessed that Putin ordered a Russian effort to manipulate the 2016 election in Trump's favor.

Rosenstein said the Russians stole and released Democratic documents after planting malicious computer codes in the network of the Democratic National Committee as well as the Democratic Congressional Campaign Committee. The Russians also illegally downloaded data related to some 500,000 voters from a state database, he charged.

While many of the indictment's details confirmed previous news reports and other assessments, it dramatically shifts the context for Trump's upcoming meeting with Putin, whom U.S. intelligence services have concluded was behind the 2016 election interference scheme. Senate Democratic leader Chuck Schumer quickly called on Trump to cancel the planned meeting.

Speaking at a press conference at Justice Department headquarters in Washington, Rosenstein said he briefed Trump about the upcoming criminal charges earlier this week. He said the indictment's timing was "a function of the collection of the facts, the evidence, and the law and a determination that it was sufficient to present the indictment at this time."

"I'll let the president speak for himself," Rosenstein told reporters when asked if Trump—who just this morning in Great Britain again blasted the Russia investigation as a "rigged witch hunt"—supported the latest step in the nearly 14-month old Mueller probe.

"Obviously it was important for the president to know what information we've uncovered because he's got to make very important decisions for the country. So he needs to understand what evidence we have for an election interference," he added.

Rosenstein added that the indictment does not allege that any U.S. citizen committed a crime, nor that "the conspiracy changed the vote count or affected any election result."

White House officials and Trump allies declared Rosenstein's statement as validating Trump's claim that there was "no collusion" between his campaign and Moscow.

"The indictments Rod Rosenstein announced are good news for all Americans," said Trump's personal lawyer, Rudy Giuliani. "The Russians are nailed. No Americans are involved. Time for Mueller to end this pursuit of the President and say President Trump is completely innocent."

"Today's charges include no allegations of knowing involvement by anyone on the campaign and no allegations that the alleged hacking affected the election result," White House spokeswoman Lindsay Walters said. "This is consistent with what we have been saying all along."

However, during a question-and-answer session with reporters, Rosenstein was more cautious. He said the lack of any claim that the hacking affected vote totals or the outcome of the election was not a conclusion on whether that happened, but rather something beyond the purview of federal prosecutors.

"We know the goal was to have an impact on the election. What impact they may have had or what their motivation may have been—independently of what's required to prove this offense—is a matter of speculation," the deputy attorney general said. "That's not our responsibility."

The indictments are the latest charges in a probe that has already netted guilty pleas from three former Donald Trump campaign aides, two of them for lying to the FBI about their contacts with Russians during or after the 2016 campaign. Mueller is also investigating the president for potential obstruction of justice, related in part to his April 2017 firing of FBI Director James Comey, who was then overseeing the federal government's burgeoning Trump-Russia probe.

Although the 11-criminal count [indictment](#) was obtained by prosecutors from Mueller's office, Rosenstein said plans are to hand the case off to Justice's National Security Division "while we await the apprehension of the defendants." That possibility seems remote—however Democrats on Friday called on Trump to demand their extradition to when he meets with Putin.

While Rosenstein stood alone on the podium five months ago when he announced another Mueller indictment of Russians alleged to have used social media to manipulate Americans during the 2016 election, on Friday he was flanked by two other officials: Assistant Attorney General for National Security John Demers and Rosenstein's top deputy, Ed O'Callaghan. Demers heads the division assigned to take over the case, while O'Callaghan has been overseeing Mueller's probe.

Mueller, who has been the focus of intense attacks and vitriol from Trump and his allies, was again absent as the new charges were announced.

Several Trump allies said they welcomed tough action against Russian election meddlers. "This is good stuff. This is what they ought to be doing," said Trump's personal lawyer John Dowd, who has often criticized Mueller's focus on Trump and his associates.

But appearing next to British Prime Minister Theresa May outside London hours before the indictment was publicly unveiled, Trump had complained that the Mueller probe has complicated his effort to befriend the Russian leader.

"I think that really hurts our country and it really hurts our relationship with Russia," he said. "I think that we would have a chance to have a very good relationship with Russia and a very good chance—a very good relationship with President Putin. I would hope so."

The indictment alleges that the Russian military officials in 2016 sent spearphishing emails to volunteers and employees of Clinton's campaign, including its chairman, John Podesta. Through those tactics, they stole user names and passwords from several people and used the information to both steal emails and hack into other Clinton campaign computers, according to the charges. The Russians allegedly funded their online hacking network with cryptocurrency.

Prosecutors say Russian officials also gained access to computer networks at the DCCC and DNC, where they covertly monitored the online activity of dozens of employees while implanting hundreds of files of malicious computer code to steal passwords and stay on their networks. The techniques allowed the Russians to get into cloud-based services in September 2016 that contained "test applications related to the DNC's analytics," the indictment says. From there, the hackers created backup files and then moved the backups to other cloud accounts the hackers controlled, the charges say.

In late May and early June, the indictment adds, the Russians took "countermeasures" to maintain access to DNC and DCCC networks after the Democratic groups hired a security company to fight off the intrusions. Those measures included attempts to "delete traces of their presence on the DCCC network using the computer program CCleaner. They also spent seven hours trying to reactive a hacking tool known as "X-Agent" that the security company had disabled, according to the indictment.

According to the indictment, the Russians employed a wide variety of tactics, including the creation of a fake website that mimicked the progressive [ActBlue.com](https://actblue.com) with the goal of siphoning contributions from Democratic donors. The Russians allegedly used stolen login credentials to insert the fraudulent link on the Democratic Congressional Campaign Committee's website, where donors would click on it.

On April 6, 2016, the Russians allegedly sought to access the emails of more than 30 Clinton campaign officials, creating a fake email address that nearly matched one of the campaign officials and including an attachment that appeared to be about Clinton's poll numbers.

"In fact this link directed the recipients' computers to a GRU-created website," the indictment alleges.

The charges filed in U.S. District Court in Washington against the Russians include criminal conspiracy to commit offense against the U.S. through cyber operations and attempting to hack into state election officials, aggravated identity theft and money laundering.

Democrats have [long speculated](#) that Moscow received guidance from Americans, possibly even ones within the Trump campaign, about how to which political targets to exploit and what kinds of leaked information would most resonate with swing voters.

Key figures close to Trump—including his son Donald Trump Jr. and his former political adviser Roger Stone—have admitted to communicating with Kremlin-linked individuals and WikiLeaks, the group that posted many of the Democrats' hacked emails.

The indictment describes communications between an unnamed person and Guccifer 2.0, an online persona the indictment calls a cover for the GRU hackers. Guccifer 2.0 released tens of thousands of emails through DC Leaks and Wikileaks, per the indictment.

After Guccifer 2.0 posted the stolen documents, the persona contacted a person identified in the indictment as "a person who was in regular contact with senior members of the presidential campaign of Donald J. Trump." The communications match [text messages](#) to and from Stone that have been previously reported and which Stone himself, who says he did nothing wrong, posted on his personal website.

Mueller's prior indictments have also revealed that George Papadopoulos, a Trump campaign foreign policy aide who pleaded guilty to lying to the FBI, was told by a Kremlin-linked professor that the Russian government had "dirt" on Clinton in the form of "thousands of emails" a full three months before the DNC hack became public.

Mueller has also indicted Russian Internet "trolls," not directly employed by the Russian government, for using fake American personas to communicate with "unwitting" Trump aides and U.S. individuals as they gathered information on the American political landscape.

While lawyers for one of the Russian companies fighting Mueller's earlier charges has pushed back in federal court, It's still considered unlikely any of the latest spate of charged hackers will actually end up in a U.S. court.

But American officials see indictments of overseas hackers as a way of shaming foreign governments. In recent years, the Justice Department has similarly filed charges against Chinese and Iranian officials for cyber intrusions.

Even before the indictments landed, Trump said he would raise with Putin the issue of Russian election interference. He has done so at least once before, during the leaders' first meeting in at the G20 summit in Hamburg, Germany last July.

After that meeting, Trump reported that Putin had denied the charges, and Trump publicly declared that it was "time to move forward." Russia's foreign minister separately claimed that that Trump "accept[ed]" Putin's insistence that the Russian government did not meddle in the election.

Trump has often cast doubt on whether Russia meddled in the election at all. During a 2016 presidential debate with Clinton, he said the election meddling could have been the work of China or even "somebody sitting on their bed, that weighs 400 pounds."

The DNC was first breached in the summer of 2015, according to CrowdStrike, the cyber firm hired by the committee after the digital break-in.

The culprit, the firm said, was "Cozy Bear," a Russian intelligence-linked hacker group that had previously infiltrated the White House and State Department. The FBI first reached out to the DNC in September to alert staffers that they were under digital siege. But the tech-support contractor that picked up the phone thought it might be a prank and the committee didn't follow through. That allowed the Russians free rein to explore DNC servers, collecting login credentials and lifting private emails and documents.

The following April, another group, the Russian military-aligned "Fancy Bear," joined its counterpart, apparently without any coordination between the two. Fancy Bear started collecting much of the same information, according to researchers.

Weeks later, the DNC caught on to the digital rummaging — and it quickly dawned on officials that they might have a catastrophe on their hands. In June, the DNC went public, blaming Russia for the digital espionage.

But what came next caught everyone — including counterintelligence veterans — off guard. The day after the DNC revealed it had been compromised, an online persona that went by the name Guccifer 2.0 popped up, claiming to be the DNC hacker and posting a sampling of documents stolen from the committee's servers.

What first appeared to be a confusing oddity quickly became a dominant force in the 2016 election. Guccifer 2.0 proceeded to disseminate reams of documents, shopping them to journalists and bloggers around the country in an effort to destabilize both local and national elections. Other mysterious websites, such as [DCLeaks.com](https://dclinks.com), suddenly appeared, posting caches of purloined emails and documents that the media eagerly consumed and converted into splashy headlines. WikiLeaks, the pro-transparency activist group, also started posting stolen DNC emails in July.

Separately, the Clinton campaign was rocked by its own data breach. In March 2016, Russian hackers infiltrated campaign chairman John Podesta's personal Gmail account, gaining access after Podesta clicked on a link in a fake email instructing him to change his password.

Six months later, WikiLeaks started Podesta's entire Gmail catalogue online in small, daily batches.

Two months after the 2016 election, a declassified [report](#) issued by the CIA, FBI and NSA — at President Barack Obama's request — stated with "high confidence" that Russian military intelligence had used the Guccifer 2.0 persona, [DCLeaks.com](https://dclinks.com) and WikiLeaks to release its hacked documents.

The leaks had a quick political impact: In July 2016, Florida Rep. Debbie Wasserman Schultz [resigned](#) as DNC chairwoman after the party's national convention, a casualty of a batch of 20,000 stolen emails posted on WikiLeaks that suggested bias against the political committee against Clinton's primary rival, Bernie Sanders.

Trump gleefully spotlighted the Democratic divide. And while Sanders publicly made amends with Clinton, the leaks fueled lingering [suspicion](#) among his supporters, some of whom post-election [studies](#) and [polls](#) show stayed home that November or even voted for Trump.

The Clinton campaign leaks also became a regular subject in the American media, which picked up on everything from portions of Clinton's private speeches to Wall Street bankers to Podesta's recipe for "creamy" risotto. The omnipresent headlines distracted and demoralized Clinton's team.

Trump reveled in the chaos. "I love WikiLeaks!" he proclaimed at one October 10 rally, waving paper copies of hacked emails in the air. "This WikiLeaks is like a treasure trove!" he said later that month.

Clinton supporters also say the leaked Podesta emails blunted the fall out from two bombshell news stories that were damaging for Trump. WikiLeaks' first post of Podesta's communications came just half an hour after The Washington Post released the "Access Hollywood" videotape of Trump bragging about sexually assaulting women. That same day, the Obama administration took the unprecedented step of [accusing](#) Russia of deploying its hackers to meddle with the U.S. election.

"WikiLeaks is unfortunately now practically a fully owned subsidiary of Russian intelligence," Clinton [told](#) an Australian broadcaster a week after the Podesta emails started appearing on the site.

Still, WikiLeaks founder Julian Assange [insisted](#) there was "no proof" Russia was behind the stolen documents that ended up on his website.

In a statement on Friday, Wasserman Schultz applauded the latest Mueller indictments. "The Democratic National Committee was the first major target of the Russian attack on our democracy, and I strongly believe that every individual who helped carry it out—foreign or domestic—should be held accountable to the fullest extent of the law," she said. "I'm pleased that the Justice Department is following the facts wherever they may lead, despite Donald Trump's dangerous distortions and his refusal to acknowledge the conclusions reached by the American Intelligence Community."

[Mueller Probe Indicts 12 Russians in Hacking of DNC and Clinton Campaign](#)

WSJ July 14th, 2018

Case 4:20-cv-00467-SDJ-CAN Document 69-2 Filed 09/27/22 Page 61 of 249 PageID #: 1903
Special counsel Robert Mueller charged a dozen Russian intelligence officers on Friday with hacking the computers of Democratic organizations and ensuring the pilfered information became public, putting Russia's interference in the 2016 election front and center as President Donald Trump [prepares to meet President Vladimir Putin](#) in Helsinki.

The detailed 29-page [indictment](#), which identified the alleged operatives by name and rank, is the latest set of charges in Mr. Mueller's wide-ranging investigation into the Kremlin's electoral meddling.

Mr. Trump, who has expressed skepticism that Russia was involved in the hacking, told reporters before the indictment that he planned to raise the issue with Mr. Putin.

[In a tweet Saturday morning](#) issued from his golf resort in Scotland, Mr. Trump faulted the Obama administration for the Russian hacking alleged in the indictment.

"The stories you heard about the 12 Russians yesterday took place during the Obama Administration, not the Trump Administrations," he wrote. "Why didn't they do something about it, especially when it was reported that President Obama was informed by the FBI in September, before the Election?"

Mr. Obama in September confronted Mr. Putin over election meddling.

The indictment lays out a vivid picture of a powerful nation deploying [the latest technological trickery](#) in a secretive effort to subvert the U.S. election. It also outlines notable details, including the way operatives allegedly used false Google security alerts to hoodwink Democratic staffers or created emails that differed by one letter from the name of a staffer of Democratic candidate Hillary Clinton.

Russia doesn't extradite its citizens to face trial in the U.S., so the defendants aren't likely to see the inside of an American courtroom, though they may be restricted in their ability to travel. Rather, the document lays out a broad case that the Russian government directed an array of crimes as it sought to disrupt the 2016 campaign.

In announcing the case, Deputy Attorney General Rod Rosenstein cited the deep partisan divide in the U.S. between Republicans and Democrats, and encouraged Americans to assess the charges on their merits and not through a political lens.

"The Internet allows foreign adversaries to attack America in new and unexpected ways," Mr. Rosenstein said. "Our response must not depend on who was victimized."

A White House spokeswoman noted that the indictment cited no wrongdoing by Americans and didn't allege that any votes were affected. "This is consistent with what we have been saying all along," spokeswoman Lindsay Walters said.

Russia on Friday repeated its previous denials of electoral meddling, saying the indictment was designed to "spoil the atmosphere" of the Trump-Putin meeting.

Democrats urged Mr. Trump to cancel the summit and refrain from meeting Mr. Putin until Russia takes responsibility and pledges to refrain from future election interference. They were joined by Sen. John McCain (R., Ariz.), who said on Twitter that "if President Trump is not prepared to hold Putin accountable, the #HelsinkiSummit should not move forward."

The indictment depicted a determined effort by two units of the Kremlin's intelligence directorate, called the GRU, to steal tens of thousands of emails and documents from Mrs. Clinton's campaign and Democratic groups, distribute them through fake online personas and pay for it through mining digital currency. Two of the defendants were also accused of hacking computers of those responsible for administering elections, including secretaries of state.

According to the indictment, the Russian officers targeted more than 300 people associated with the Clinton campaign, the Democratic Congressional Campaign Committee and the Democratic National Committee, luring them with fake emails.

The hackers sent such a “spear-phishing” email to Mr. Podesta on March 19, 2016. Mr. Podesta followed the fake security instructions in the message, giving the hackers the ability to steal more than 50,000 of his emails, the indictment said.

Meanwhile, the officers were also targeting the DCCC, and obtained the credentials of one employee to access the network. That gave them access to at least 10 computers and the ability to monitor employees’ computer activity and steal passwords. Using that information, they successfully hacked into the DNC computers, ultimately gaining access to 33 DNC computers.

Once inside the network, Russian operatives demonstrated a focused effort to find files on particular topics, the indictment said. Shortly after breaching the DCCC in April 2016, the alleged conspirators searched for files that included the words “hillary,” “trump” or “cruz.” A folder labeled “Benghazi Investigations” was also copied, the indictment said.

This was around the time that Trump foreign policy adviser George Papadopoulos learned that Russia possessed “dirt” on Mrs. Clinton, according to documents filed in connection with [his plea agreement with Mr. Mueller’s team](#).

By May 2016, the Democratic groups hired a cybersecurity company to address the breach, but the GRU officers continued to try to maintain their access to the networks, and remained on the DNC network until October 2016, the indictment said.

On July 27, 2016, the officers tried for the first time to spear-phish email accounts used by Mrs. Clinton’s personal office, the indictment said. Earlier that day, Mr. Trump had invited Russia to unearth missing emails from her time as secretary of state, telling reporters, “Russia, if you’re listening, I hope you’re able to find the 30,000 emails that are missing.”

The indictment alleges that two of the main conduits of the stolen data, Guccifer 2.0 and DCLeaks, were created by the Russian government. Guccifer 2.0 claimed to be a lone Romanian hacker, which the indictment alleges was intended to “undermine allegations of Russian responsibility for the intrusion.”

The Russians later began funneling information to “Organization 1,” which isn’t named in the indictment but is identifiable as Wikileaks.org, which published thousands of emails belonging to Mr. Podesta and the DNC.

In August 2016, the Russian officers posing as Guccifer 2.0 communicated with a person “who was in regular contact” with “senior members” of the Trump campaign, telling the person, “please tell me if i can help u anyhow...it would be a great pleasure to me.” The indictment doesn’t name the person, but former Trump adviser Roger Stone has posted on his website a text exchange with Guccifer that corresponds to language included in the indictment.

Eleven of the GRU officials are charged with conspiring to commit computer crimes, launder money and commit identity theft through the DNC and Clinton hacks. One of the officers, along with a 12th individual, were also accused of trying to hack into state election agencies and voting software companies.

Specifically, “Russian GRU officers hacked the website of a state election board and stole information about 500,000 voters,” Mr. Rosenstein said. There is no allegation that information was used to alter vote totals.

Case 4:20-cv-00467-SDJ-CAN Document 69-2 Filed 09/27/22 Page 63 of 249 PageID #: 1905
Friday's indictment follows previous election-interference accusations Mr. Mueller has leveled at Moscow. In February, a federal grand jury indicted [three Russian companies and 13 Russian citizens](#) on charges of engaging in a widespread effort to meddle in the 2016 campaign through social-media messages, invented fake personas and staged rallies.

Before Friday's indictment, Mr. Mueller's office had publicly filed cases against 20 people and three companies, and had obtained five guilty pleas, including from Mr. Trump's first national security adviser, Michael Flynn. [Mr. Flynn pleaded guilty last year](#) to lying to the FBI about his communications with the Russian ambassador to the U.S.

Director of National Intelligence Dan Coats, speaking about Russian cyber influence at the Hudson Institute think tank shortly after the indictment was released, said U.S. intelligence agencies continue to see Russia attempting to create new social media accounts that pose as Americans in order to inflame political and social divisions.

Intelligence agencies haven't yet seen Russia attempt to hack election infrastructure as it did in the 2016 election, Mr. Coats said. "However," he added, "we fully realize that we are one click away from a similar situation repeating itself."

U.S. accuses Russian spies of 2016 election hacking as summit looms

Reuters July 13th, 2018

WASHINGTON (Reuters) - A federal grand jury charged 12 Russian intelligence officers on Friday with hacking Democratic computer networks in 2016, in the most detailed U.S. accusation yet that Moscow meddled in the presidential election to help Republican Donald Trump.

The indictment, which alleges a wide-ranging conspiracy involving sophisticated hacking and staged releases of documents, raises the stakes for a summit next week between President Trump and Russian President Vladimir Putin.

Officers of Russia's military intelligence agency, the GRU, covertly monitored computers of Democratic candidate Hillary Clinton's campaign and Democratic campaign committees, and stole large amounts of data, the indictment said.

"In addition to releasing documents directly to the public, the defendants transferred stolen documents to another organization, not named in the indictment, and discussed timing the release of the documents in an attempt to enhance the impact on the election," Deputy U.S. Attorney General Rod Rosenstein told a news conference.

Friday's indictment was secured by Special Counsel Robert Mueller as part of his probe into Russian involvement in the election. It was the first by Mueller that directly charges the Russian government with meddling in the election, which Trump unexpectedly won. The Kremlin denies it interfered.

Rosenstein said he briefed Trump this week about the indictment. It contains no allegations that U.S. citizens committed a crime, he said.

A few hours before the indictments were announced, Trump called the Mueller investigation a "rigged witch hunt" that is hurting the United States' relationship with Russia.

The announcement of the indictment came at an awkward time for Trump, who met Britain's Queen Elizabeth at Windsor Castle on Friday for tea during a visit to Britain.

Trump said he would "absolutely, firmly ask" Putin about the meddling at their planned meeting in Helsinki on Monday.

The Russian Foreign Ministry said on Friday that the indictment aimed to damage the atmosphere before the summit. It said there was no evidence that the 12 people charged were linked to military intelligence or hacking.

Several prominent Democratic lawmakers called on Trump to cancel the summit.

“In light of this stunning indictment by the Justice Department that these Russian conspirators attacked our democracy and were communicating with Americans to interfere in our election, President Trump should immediately cancel his meeting with Vladimir Putin,” said Senator Jack Reed, the ranking Democrat on the Senate Armed Services Committee.

PROPAGANDA, HACKING

Mueller is investigating whether Trump’s campaign colluded with Russia and whether the president has unlawfully sought to obstruct the Russia investigation.

U.S. intelligence agencies concluded in January 2017 that Russia, in action ordered by Putin, used propaganda and hacking to meddle in the election to harm Clinton and eventually help Trump.

But the 29-page document describes several incidents in which the alleged Russian hackers, using the internet personas DCLeaks and Guccifer 2.0, were in contact with Americans.

It says Russian operatives provided direct assistance to a candidate for the U.S. Congress, who in August 2016 requested and received from Guccifer 2.0 documents stolen from the DCCC about their opponent. The candidate and the person’s party affiliation were not identified.

That same month, the indictment says, “the Conspirators, posing as Guccifer 2.0, sent a reporter stolen documents pertaining to the Black Lives Matter movement,” which was a sensitive political issue for the Democratic Party.

Deputy U.S. Attorney General Rod Rosenstein announces grand jury indictments of 12 Russian intelligence officers in special counsel Robert Mueller's Russia investigation during a news conference at the Justice Department in Washington, U.S., July 13, 2018. REUTERS/Leah Millis

The reporter, who was not identified, “responded by discussing when to release the documents and offering to write an article about their release.”

The indictment says the Russian operatives wrote to a unnamed person “who was in regular contact with senior members” of the Trump campaign. Trump ally Roger Stone told CNN he “probably” was the person referred to in the indictment.

The indictment says the Russian operatives told the person it would be a “great pleasure” to help them and later asked their opinion about a stolen DCCC document posted online. “(P)retty standard,” the person responded.

Stone denied passing any stolen emails to WikiLeaks. He said in a statement to Reuters: “The indictments today show I did not conspire with any of the defendants to do the hacking, distribute the stolen emails or aid them in anyway.”

“RUSSIANS ARE NAILED”

A former federal prosecutor, Renato Mariotti, raised the question of the next steps in the probe.

“The open question is whether Americans were involved in this and will they be charged. You can certainly imagine a subsequent indictment in the future of an American of being part of this conspiracy,” Mariotti said.

The indictment says that on or about July 27, 2016, the Russians attempted for the first time to break into email accounts “at a domain hosted by a third-party provider and used by Clinton’s personal office. At or around the same time, they also targeted 76 email addresses at the domain of the Clinton Campaign.”

The same day, candidate Trump told a news conference: “Russia if you are listening I hope you’re able to find the 30,000 (Clinton) emails that are missing,” referring to emails from a private server used by Clinton when she was secretary of state.

The indictment documents extensive cooperation between the Russian hackers and the unnamed “Organization 1.”

That group appears to match WikiLeaks, which released large numbers of hacked Democratic Party emails during the 2016 campaign.

On July 22, 2016, Organization 1 “released over 20,000 emails and other documents stolen from the DNC network by the Conspirators,” the indictment said. That matches the date that a WikiLeaks began publishing internal DNC documents.

WikiLeaks, which was not indicted, did not immediately respond to a request for comment.

In June 2016, “Organization 1 sent a private message to Guccifer 2.0 to ‘(s)end any new material (stolen from the DNC) here for us to review and it will have a much higher impact than what you are doing,” the indictment said.

Trump lawyer Rudolph Giuliani, in a tweet, said the indictments showed it was time to end the special counsel’s probe.

“The indictments Rod Rosenstein announced are good news for all Americans. The Russians are nailed. No Americans are involved. Time for Mueller to end this pursuit of the President and say President Trump is completely innocent,” Giuliani said.

Mueller has secured indictments against several former Trump campaign aides, including former campaign chairman Paul Manafort and former White House national security adviser Michael Flynn.

In February, Mueller charged 13 Russians and three Russian companies in an elaborate conspiracy to interfere in the election. That indictment said the Russians adopted false online personas to push divisive messages, traveled to the United States to collect intelligence and staged political rallies while posing as Americans.

[Russian Intelligence Officers Have Been Indicted For Hacking Hillary Clinton's Presidential Campaign](#)

BuzzFeed News July 13th, 2018

Twelve Russian military officers were [indicted Friday](#) by a federal grand jury for hacking Hillary Clinton's presidential campaign and two Democratic organizations — marking the latest charges to come out of special counsel Robert Mueller's investigation.

The defendants, all members of the Russian intelligence agency GRU, are accused of conspiring to hack into computer networks, steal documents, and orchestrate their release with the goal of interfering with the 2016 presidential election.

Although the Russian defendants communicated with unnamed Americans, according to the indictment, there is no allegation in the charging papers that any American citizen knew they were participating in unlawful activity or that they were communicating with Russian intelligence. The charging papers indicate

The indictment also alleges a scheme to hack into state government networks to steal voter information. According to charging papers, hackers stole the personal information of more than 500,000 voters from the website of an unidentified state board of elections, including names, addresses, partial Social Security numbers, birthdates, and driver's license numbers. The indictment doesn't specify what happened to that information, and Deputy Attorney General Rod Rosenstein did not elaborate when asked about it on Friday. Rosenstein said there was no evidence that the alleged criminal activity affected vote counts or election outcomes.

At a press conference on Tuesday announcing the indictment, Rosenstein warned against public speculation about federal investigations.

"I want to caution you that people who speculate about federal investigations usually do not know all of the relevant facts. We do not try cases on television or in congressional hearings. Most anonymous leaks are not from the government officials who actually conduct investigations," Rosenstein said in prepared remarks. "We follow the rule of law, which means that we follow procedures and reserve judgment. We complete our investigations and evaluate all of the evidence before we reach any conclusion."

Rosenstein said he had briefed President Donald Trump about the indictment. Asked about Trump's repeated characterization of Mueller's investigation as a "witch hunt," Rosenstein said he could only comment on the evidence. When charges are filed, he said, they represent "a determination by prosecutors and agents, without regard to politics, that we believe the evidence is sufficient to justify the charges."

Although the case came out of Mueller's investigation, Rosenstein said it would be transferred to the Justice Department's National Security Division.

Mueller's investigation is ongoing, Rosenstein said Friday. White House spokesperson Lindsay Walters put out a statement highlighting Rosenstein's comments that no Americans were accused of criminal activity and that there was no allegation that votes were affected.

"Today's charges include no allegations of knowing involvement by anyone on the campaign and no allegations that the alleged hacking affected the election result. This is consistent with what we have been saying all along," Walters said.

Responding to news of the latest charges, Trump's personal lawyer Rudy Giuliani [tweeted](#), "Time for Mueller to end this pursuit of the President and say President Trump is completely innocent."

The charges come as Trump will meet face-to-face with Russian President Vladimir Putin in Finland on Monday. Trump has in the past defended Russia and said he believes Putin when Putin said he didn't meddle in the election.

"I don't think anybody knows it was Russia that broke into the DNC. She's saying Russia, Russia, Russia. Maybe it was. I mean, it could be Russia, but it could also be China, but it could also be lots of other people, it also could be someone sitting on their bed that weighs 400 pounds, OK?" Trump said in September 2016.

In a brief, hastily organized press conference, Sen. Mark Warner, the ranking member of the Senate Intelligence Committee, commended the Mueller investigation, which he said had resulted in "direct evidence of Russian agents interfering in our elections." He said a "vast majority" of the information from today was new, at least to that level of specificity, and he stated his surprise at the information.

"What is remarkable about special prosecutor Mueller's work was the level of specificity to identify the actual Russian spies who specifically interfered in our state's election systems, who hacked into the DNC, who hacked into the Democratic Congressional Campaign Committee, who hacked into John Podesta's

Case 4:20-cv-00467-SDJ-CAN Document 69-2 Filed 09/27/22 Page 67 of 249 PageID #: 1909
emails. That's pretty good investigation work by Mueller and his team," Warner said. He spent time criticizing the White House's attitude toward Russia, and called on Trump to stop taking one-on-one meetings with Putin, expressing a fear that Trump could be taken advantage of.

According to the indictment, as of at least March 2016 the GRU officers had launched a sustained effort to hack into the computer networks of the DNC, Clinton's campaign, and the Democratic Congressional Campaign Committee. That included hacking the email account of Clinton's campaign chair, John Podesta.

Within months, the defendants are accused of having staged the release of tens of thousands of stolen documents. According to the indictment, the officers registered a domain, DCLeaks.com, and created the "fictitious persona" Guccifer 2.0, to facilitate the release of documents. When the DNC announced it had been hacked in June 2016, prosecutors say the defendants created Guccifer 2.0 to falsely make it seem as though it was the work of a single Romanian hacker. They also allegedly used the Guccifer 2.0 persona to release documents through the website of an additional unnamed entity, referred to as "Organization 1."

According to the indictment, the defendants, through the Guccifer 2.0 persona, communicated with an unidentified person "who was in regular contact with senior members" of the Trump campaign, asking what they thought about the released documents and offering to send information. The charging papers also alleged that the defendants, via Guccifer 2.0, also communicated with an unnamed US congressional candidate, a state lobbyist, and a reporter.

The indictment alleges that the GRU officials used spear-phishing to target volunteers and employees of Clinton's campaign. They allegedly were able to steal the usernames and passwords of numerous individuals, and then use those credentials to steal emails and maintain access. The defendants allegedly sent Podesta a "spoofing" email that was made to look like a security notification from Google, instructing the recipient to click on a link. According to the indictment, the hackers stole more than 50,000 emails from Podesta's account.

Once the hackers had access to the DCCC network, they allegedly searched one computer for the terms "hillary," "cruz," and "trump," copied a folder called "Benghazi Investigations," and targeted computers with opposition research and 2016 field operations information.

During his news conference, Rosenstein spoke about the nonpartisan nature of the investigation.

"When we confront foreign interference in American elections, it's important for us to avoid thinking politically as Republicans or Democrats and instead to think patriotically as Americans," Rosenstein said. "Partisan warfare fueled by modern technology does not fairly reflect the grace, dignity, and unity of the American people."

"Our response must not depend on which side was victimized," he said.

When asked about the timing of the indictment, days before Trump is scheduled to meet with Putin, Rosenstein said, "The timing, as I mentioned, is a function of the collection of the facts, the evidence, and the law."

The defendants are Russian nationals, and assuming they don't travel to the United States or otherwise participate in the US litigation, it will be difficult for the Justice Department to pursue the charges against them. The pending case could make it difficult for them to travel internationally, and could make them subject to the US sanctions.

This is the second case brought by Mueller's office against a group of Russian nationals accused of attempting to interfere in the 2016 election. In February, a grand jury returned an indictment against the Russian-based troll farm Internet Research Agency, two other Russian entities, and [13 Russian individuals](#) accused of creating fake US personas to manage social media accounts and collect intelligence.

Only one of the defendants in that case, Concord Management and Consulting, has engaged in the case to date. Concord has [pleaded not guilty](#) and is contesting the legitimacy of Mueller's appointment.

This is the ninth case brought by Mueller's office. It was filed in the US District Court for the District of Columbia, and assigned to US District Judge Amy Berman Jackson — the same judge presiding over one of the special counsel office's prosecutions against former Trump campaign chair Paul Manafort.

No one from Trump's campaign has been charged with colluding with the Russian government, but prosecutors have connected people involved in the campaign and Russia-affiliated individuals in court papers. Alex van der Zwaan, a Dutch lawyer, pleaded guilty earlier this year to lying to investigators about his contacts with former deputy Trump campaign chair Rick Gates — who had been Manafort's co-defendant but has since pleaded guilty and agreed to cooperate — and an unnamed person known as "Person A." According to a [March filing by prosecutors](#), Gates told van der Zwaan that Person A, who Gates was in touch with in 2016, was a former Russian intelligence officer with GRU; the FBI assessed that Person A still had ties to Russian intelligence in 2016.

Media reports speculated that Person A was Konstantin Kilimnik, a longtime Russian-Ukrainian business partner of Manafort; Kilimnik has denied ties to Russian intelligence. In June, Kilimnik became Manafort's new co-defendant — Mueller's office [charged him](#) with attempting to interfere with potential witnesses.

Two civil lawsuits have made the jump in connecting the DNC hack to the Trump campaign, alleging a conspiracy with the Russian government. One, filed last year in DC federal court on behalf of two DNC donors and a former DNC employee, was dismissed earlier this month after a judge found it was filed in the wrong jurisdiction; the judge did not rule on the substance of the allegations. The plaintiffs refiled the case this week in the US District Court for the Eastern District of Virginia.

In April, the DNC filed a [lawsuit](#) of its own in federal court in Manhattan in April. That case is pending.

The Coincidence at the Heart of the Russia Hacking Scandal

The Atlantic July 13th, 2018

The [broad outlines of Friday's indictment](#) by Special Counsel Robert Mueller, charging 12 Russians with conspiracy, identity theft, and money laundering in connection with hacking during the 2016 presidential election, are not surprising. The hacking of the Democratic National Committee has been public knowledge [since July 2016](#), and even then, the authorities publicly stated that the perpetrators were Russian government officials. Other details, such as the apparent involvement of WikiLeaks and Trump adviser Roger Stone, were also known. Some of the details, however, are striking.

On July 27, 2016, at a Trump [press conference in Florida](#), the candidate referred to 33,000 emails that an aide to Hillary Clinton had deleted from the former secretary of state's personal email server. The DNC had recently announced the Russian intrusion, and Trump speculated that if Russia broke into the DNC, it would have accessed Clinton's emails, too.

"By the way, if they hacked, they probably have her 33,000 emails," Trump said. "I hope they do. They probably have her 33,000 emails that she lost and deleted. Because you'd see some beauties there."

That was perhaps irresponsible speculation, but it wasn't crazy. There were widespread questions about Clinton's information security, and whether she might have compromised government secrets. But a few minutes later Trump said something much stranger.

"I will tell you this: Russia, if you're listening, I hope you're able to find the 30,000 emails that are missing," he said. "I think you will probably be rewarded mightily by our press."

The president was encouraging a foreign adversary to illegally hack into messages by a former secretary of state that might contain sensitive information, then release them publicly.

Trump had good reason to believe that Russia *was* listening. The previous month, his son, Donald Jr.; son-in-law, Jared Kushner; and campaign chairman, Paul Manafort, had a meeting at Trump Tower with Russians who they believed were offering damaging information about Clinton. (The meeting wasn't revealed to the public until 2017, and both the Russians and the Trump campaign officials say no dirt was exchanged.) Prior to the meeting, Trump Jr. had [received an email](#) stating that the meeting was "part of Russia and its government's support for Mr. Trump."

Mueller's [indictment](#) offers new evidence that Russia was listening—and acting on Trump's request. The indictment charges 12 officers of the GRU, Russia's military-intelligence agency, with hacking intended to interfere with the election. [According to the document](#):

The Conspirators spearphished individuals affiliated with the Clinton Campaign throughout the summer of 2016. For example, on or about July 27, 2016, the Conspirators 7 attempted after hours to spearphish for the first time email accounts at a domain hosted by a third-party provider and used by Clinton's personal office. At or around the same time, they also targeted seventy-six email addresses at the domain for the Clinton Campaign.

In other words, a Russian attempt to penetrate Clinton's server and her campaign came around the same time that Trump was publicly pleading with Russia to do just that. (Mueller alleges that there had been attempts to hack Clinton's campaign since at least March 2016.)

Trump's hacking request was so egregious that it earned immediate pushback from other Republicans. Speaker Paul Ryan's spokesman issued a statement [saying](#), "Russia is a global menace led by a devious thug. Putin should stay out of this election." Even Mike Pence, Trump's own vice-presidential nominee, contradicted his running mate. "If it is Russia [that hacked the DNC] and they are interfering in our elections, I can assure you both parties and the United States government will ensure there are serious consequences," [he said](#).

The indictment notes other examples of Russia releasing documents at times engineered to benefit the Trump campaign, though it doesn't offer any evidence that Trump aides directed, or were aware of, those releases before they happened. The indictment notes that WikiLeaks released a tranche of emails allegedly stolen by Russia on July 22, 2016—just three days before the DNC, a convenient stroke of timing for Trump. Then, on October 7, 2016, WikiLeaks released another batch of hacked emails within hours of the revelation of the *Access Hollywood* tape, in which Trump is overheard boasting about sexually assaulting women.

In a [statement](#) responding to the indictment on Friday, the White House did not condemn Russian interference in the election, instead striking a purely defensive note regarding the president's 2016 victory. "Today's charges include no allegations of knowing involvement by anyone on the campaign and no allegations that the alleged hacking affected the election result," a spokeswoman said. "This is consistent with what we have been saying all along." Trump is scheduled to meet one-on-one with Russian President Vladimir Putin on Monday in Helsinki, Finland.

At the time of Trump's comments in July 2016, it was easy to write them off as the latest sideshow from his circus of a campaign. Though he was at that moment enjoying a brief post-Republican National Convention [bounce in the polls](#), Trump was widely expected to lose the election, so his comments, while dangerous, were of limited relevance.

That was incorrect, of course: Trump defeated Clinton. And since then, the public has learned a great deal about both Russian interference in the election and ties between the Trump campaign and Russia.

Case 4:20-cv-00467-SDJ-CAN Document 69-2 Filed 09/27/22 Page 70 of 249 PageID #: 1942
Mueller indicted a coterie of Russians on charges of interfering in the election via online trolling. The public learned of the June 2016 Trump Tower meeting, despite multiple attempts by Trump Jr. to mislead about it. Former National-Security Adviser Michael Flynn pleaded guilty to lying to the FBI about contacts with the Russian ambassador. Former Trump campaign foreign-policy adviser George Papadopoulos pleaded guilty to lying to the FBI about contacts with Russians during the election. Another foreign-policy aide, Carter Page, offered confusing and sometimes contradictory evidence about his travels to Russia and elsewhere. Mueller has produced evidence showing Manafort's deep pre-campaign ties to the Kremlin. Kushner reportedly attempted to establish a back-channel to communicate with Russia. [And so on.](#)

[As I have argued](#), the question of whether these ties existed ought to be closed. There is extensive evidence to support that they did. Friday's indictment adds an astonishing new wrinkle. Trump campaign officials may or may not have been colluding with a Russian influence operation behind closed doors, but Trump himself was making no attempt to hide his own desires, with cameras and reporters watching. The Russians heeded his call.

Mueller's Politicized Indictment of Twelve Russian Intelligence Officers

National Review July 16th, 2018

So, is Russia now presumed innocent of hacking the 2016 election?

If not, it is difficult to understand any proper purpose served by Special Counsel Robert Mueller's [indictment](#) of twelve military officers in the Kremlin's intelligence services for doing what everybody in America already knew that they did, and has known since before Donald Trump took office — indeed, since before the 2016 election.

Make no mistake: This is nakedly politicized law enforcement. There is absolutely no chance any of the Russian officials charged will ever see the inside of an American courtroom. The indictment is a strictly political document by which the special counsel seeks to justify the existence of his superfluous investigation.

Oh, and by the way, the answer to the question posed above is, “Yes, it is now the official position of the United States that Russia gets our Constitution's benefit of the doubt.” Here is Deputy Attorney General Rod Rosenstein [announcing](#) the Friday the 13th indictment: “In our justice system, everyone who is charged with a crime is presumed innocent unless proven guilty.”

Of course, the indicted Russians are never going to be proven guilty — not in the courtroom sense Rosenstein was invoking.

As is so often the case in today's politicized Justice Department, Rosenstein was trying to make a different political point. As he went on to note, if people whom we have formally charged are presumed innocent, then, *a fortiori*, people who have not been accused — implicitly, Rosenstein was talking about President Trump — must also be presumed innocent. But, see, you can't make that point without stepping on the political purpose of Friday's charade: We have taken the not only pointless but reckless step of *indicting* operatives of a hostile foreign power who cannot be prosecuted and whose schemes could easily have been exposed — and, in fact, *have* been exposed, multiple times — in public government reports; so now, due-process rules oblige us to caution you that we must presume the Russians did not do what we have formally accused them of doing. They are entitled to that presumption unless and until we convict them in court . . . which is never going to happen.

Rosenstein made another telling remark at his big press conference. The Justice Department, he explained, will now “transition responsibility for this case to our Department's National Security Division while we await the apprehension of the defendants.”

Now, stop giggling over that last part — the bit where we hold our breath until Russian dictator Vladimir Putin extradites his spies into the FBI’s waiting arms. I’m talking about the first part: Mueller’s case, *the definitive case about what Russia did to interfere in the 2016 election*, is no longer Mueller’s case. It is being “transitioned” — i.e., buried — in the Justice Department unit that deals with counterintelligence matters that do not result in public trials.

This underscores what we have been arguing here since before Mueller was appointed: There was no need and no basis in federal regulations for a special counsel.

A special counsel is supposed to be appointed only when there are (a) a concrete factual basis to believe federally prosecutable crimes have been committed, calling for a criminal investigation, and (b) a conflict of interest that prevents the Justice Department from conducting the criminal investigation.

As we’ve observed countless times, there was no basis for a criminal investigation of President Trump or the Trump campaign. The fact that Russia interfered in an American election — as it routinely does — never meant that the perceived beneficiary of the interference was criminally complicit in it. There is no known evidence that Trump-campaign officials had any involvement in hacking by the Russian intelligence services. Mueller’s new indictment powerfully suggests that this could not have happened — the Russians were expert in their cyberespionage tactics, they did not need anyone’s help, and they took pains to conceal their identity from everyone with whom they dealt.

Moreover, even though Trump-campaign officials have been charged with other crimes (having nothing to do with the 2016 election), and some of those Trump officials had “contacts” with Russians, Mueller has never charged one of them with a crime related to Russia’s espionage attack on the election, nor has he ever elicited from any defendant who pled guilty an admission of any such crime. The only known allegations of such a crime are contained in the unverified, Clinton-campaign-sponsored Steele dossier, and the Trump-campaign figures implicated in it have either not been charged at all (e.g., Carter Page, Michael Cohen), or not been charged with a “collusion” crime (Paul Manafort).

Thus, among the worst aspects of Mueller’s new indictment is its continuation of the Justice Department’s politicized perversion of its critical counterintelligence mission.

Lacking the requisite basis to conduct a criminal investigation, the Justice Department used its counterintelligence mission as a pretext for appointing a special counsel. This was grossly improper: (1) Counterintelligence work, which is geared at thwarting the operations of hostile foreign powers, is not the prosecutor work of building criminal cases; (2) not surprisingly, then, there is no authority in the regulations to assign a special counsel to a counterintelligence investigation; and (3) because counterintelligence authorities do not afford Americans the due-process protections required in criminal investigations, the Justice Department is not permitted to use counterintelligence as a pretext for conducting what is actually an effort to build a criminal prosecution.

Now Mueller has taken the next logical wayward step: He has woven an indictment that can never be tried out of counterintelligence work against foreign governments that is not supposed to be the subject of criminal prosecution — i.e., the subject of public courtroom testing under due-process rules.

This is not the way counterintelligence is supposed to work. And the Justice Department knows it. That is why Mueller’s indictment will now be the property of DOJ’s National Security Division, the home of other non-prosecutable foreign counterintelligence work that is never intended to see the light of day in a public courtroom.

And why such an easy transition? *Because there is no conflict of interest.*

There never was. Russia’s interference in the 2016 election was never something that the Justice Department was unable to investigate in the normal course. In fact, for months, *the Trump Justice Department was*

Case 4:20-cv-00467-SDJ-CAN Document 69-2 Filed 09/27/22 Page 72 of 249 PageID #: 1914
investigating it in the normal course, just as the Obama Justice Department had done. Then, President Trump fired FBI director James Comey. It was this event that prompted Rosenstein to appoint Mueller. We got a special counsel not because of Russia's espionage or any evidence indicating actual Trump-campaign complicity in it; we got a special counsel because Rosenstein was deeply involved in Comey's ouster and wanted to fend off Democratic attacks on him over it.

The only point of the new indictment is to justify Rosenstein's decision and Mueller's existence. Proponents of the unnecessary special counsel want to say, "See, we really needed this investigation." But that can be said with a straight face only if the goalposts are moved.

To be clear, we did need *an FBI counterintelligence investigation* of Russia's espionage operation against the 2016 election, and we already had a quite aggressive one before Mueller came on the scene. But we would have needed *a special-counsel investigation* only if there had been a concrete factual basis to believe the *Trump campaign conspired in Russia's espionage operation against the 2016 election*.

There never was. So now, the purported need for Mueller is being rationalized on two fictitious premises.

The first is that the new indictment shows we needed Mueller to get to the bottom of Russia's perfidy. This is false: There is nothing new in Mueller's indictment, his participation was unnecessary to discover what our counterintelligence investigators have learned, and the intelligence they have gathered should not have been put in an indictment — aggression by hostile foreign powers is not a law-enforcement issue, and it is a mockery of the justice system to charge foreign aggressors and pretend we presume them innocent of their attacks against our country.

The second is that the number of indictments Mueller has generated proves that there were solid grounds to suspect Trump-campaign "collusion" in Russia's election-meddling. The blatant, partisan dishonesty of this claim is best encapsulated in this passage from the [Washington Post's report on Mueller's new indictment](#):

Mueller and a team of prosecutors have been working since May 2017 to determine whether any Trump associates conspired with Russia to interfere in the election. With the new indictment, his office has filed charges against 32 people on crimes including hacking, money laundering and lying to the FBI.

The *Post* goes on grudgingly to point out that 26 of the 32 charged are Russians "who are unlikely to ever be put on trial in the United States." (*Unlikely?*) But the paper conveniently omits mention of the fact that *none of the 32 have been charged with a Trump–Russia conspiracy to interfere in the election*. That's the only thing Mueller was needed for.

As [I pointed out on Twitter](#) over the weekend, besides the two-dozen-odd Kremlin operatives already charged, there are 144 million other people in Russia who will never see the inside of an American courtroom. If Mueller indicts every one of them, his stats will look *really* impressive . . . and there will still be no Trump conspiracy against the election.

What there will be, though, is a new international order in which nation-states are encouraged to file criminal charges against each other's officials for actions deemed to be provocative (or, more accurately, actions that can be exploited for domestic political purposes). Of all government officials in the world, American officials are the most active on the global stage — and that includes meddling in other countries' elections. I doubt our diplomats, intelligence operatives, elected officials, and citizens will much like living in the world Robert Mueller and Rod Rosenstein have given us. If the idea was to give Vladimir Putin and his thug regime a new way to sabotage the United States, nice work.

FOR IMMEDIATE RELEASE Friday, July 13, 2018

GRAND JURY INDICTS 12 RUSSIAN INTELLIGENCE OFFICERS FOR HACKING OFFENSES RELATED TO THE 2016 ELECTION

The Department of Justice today announced that a grand jury in the District of Columbia returned an indictment presented by the Special Counsel's Office. The indictment charges twelve Russian nationals for committing federal crimes that were intended to interfere with the 2016 U.S. presidential election. All twelve defendants are members of the GRU, a Russian Federation intelligence agency within the Main Intelligence Directorate of the Russian military. These GRU officers, in their official capacities, engaged in a sustained effort to hack into the computer networks of the Democratic Congressional Campaign Committee, the Democratic National Committee, and the presidential campaign of Hillary Clinton, and released that information on the internet under the names "DCLeaks" and "Guccifer 2.0" and through another entity.

"The Internet allows foreign adversaries to attack America in new and unexpected ways," said Deputy Attorney General Rod J. Rosenstein. "Together with our law enforcement partners, the Department of Justice is resolute in its commitment to locate, identify and seek to bring to justice anyone who interferes with American elections. Free and fair elections are hard-fought and contentious, and there will always be adversaries who work to exacerbate domestic differences and try to confuse, divide, and conquer us. So long as we are united in our commitment to the shared values enshrined in the Constitution, they will not succeed."

According to the allegations in the indictment, Viktor Borisovich Netyksho, Boris Alekseyevich Antonov, Dmitriy Sergeyevich Badin, Ivan Sergeyevich Yermakov, Aleksey Viktorovich Lukashev, Sergey Aleksandrovich Morgachev, Nikolay Yuryevich Kozachek, Pavel Vyacheslavovich Yershov, Artem Andreyevich Malyshev, Aleksandr Vladimirovich Osadchuk, Aleksey Aleksandrovich Potemkin, and Anatoliy Sergeyevich Kovalev were officials in Unit 26165 and Unit 74455 of the Russian government's Main Intelligence Directorate.

In 2016, officials in Unit 26165 began spearphishing volunteers and employees of the presidential campaign of Hillary Clinton, including the campaign's chairman. Through that process, officials in this unit were able to steal the usernames and passwords for numerous individuals and use those credentials to steal email content and hack into other computers. They also were able to hack into the computer networks of the Democratic Congressional Campaign Committee (DCCC) and the Democratic National Committee (DNC) through these spearphishing techniques to steal emails and documents, covertly monitor the computer activity of dozens of employees, and implant hundreds of files of malicious computer code to steal passwords and maintain access to these networks.

The officials in Unit 26165 coordinated with officials in Unit 74455 to plan the release of the stolen documents for the purpose of interfering with the 2016 presidential election. Defendants registered the domain DCLeaks.com and later staged the release of thousands of stolen emails and documents through that website. On the website, defendants claimed to be "American hackers" and used Facebook accounts with fictitious names and Twitter accounts to promote the website. After public accusations that the Russian government was behind the hacking of DNC and DCCC computers, defendants created the fictitious persona Guccifer 2.0. On the evening of June 15, 2016 between 4:19PM and 4:56PM, defendants used their Moscow-based server to search for a series of English words and phrases that later appeared in Guccifer 2.0's first blog post falsely claiming to be a lone Romanian hacker responsible for the hacks in the

hopes of undermining the allegations of Russian involvement.

Members of Unit 74455 also conspired to hack into the computers of state boards of elections, secretaries of state, and US companies that supplied software and other technology related to the administration of elections to steal voter data stored on those computers.

To avoid detection, defendants used false identities while using a network of computers located around the world, including the United States, paid for with cryptocurrency through mining bitcoin and other means intended to obscure the origin of the funds. This funding structure supported their efforts to buy key accounts, servers, and domains. For example, the same bitcoin mining operation that funded the registration payment for DCLeaks.com also funded the servers and domains used in the spearphishing campaign.

The indictment includes 11 criminal counts:

- Count One alleges a criminal conspiracy to commit an offense against the United States through cyber operations by the GRU that involved the staged release of stolen documents for the purpose of interfering with the 2016 president election;
- Counts Two through Nine charge aggravated identity theft for using identification belonging to eight victims to further their computer fraud scheme;
- Count Ten alleges a conspiracy to launder money in which the defendants laundered the equivalent of more than \$95,000 by transferring the money that they used to purchase servers and to fund other costs related to their hacking activities through cryptocurrencies such as bitcoin; and
- Count Eleven charges conspiracy to commit an offense against the United States by attempting to hack into the computers of state boards of elections, secretaries of state, and US companies that supplied software and other technology related to the administration of elections.

There is no allegation in the indictment that any American was a knowing participant in the alleged unlawful activity or knew they were communicating with Russian intelligence officers. There is no allegation in the indictment that the charged conduct altered the vote count or changed the outcome of the 2016 election.

Everyone charged with a crime is presumed innocent unless proven guilty in court. At trial, prosecutors must introduce credible evidence that is sufficient to prove each defendant guilty beyond a reasonable doubt, to the unanimous satisfaction of a jury of twelve citizens.

This case was investigated with the help of the FBI's cyber teams in Pittsburgh, Philadelphia and San Francisco and the National Security Division. The Special Counsel's investigation is ongoing. There will be no comments from the Special Counsel at this time.

Exhibit H



U.S. Department of Justice

National Security Division

Washington, D.C. 20530

Ty Clevenger
212 S. Oxford St. #7D
Brooklyn, NY 112217

August 30, 2021

Re: FOIA/PA #20-333

Dear Mr. Clevenger:

This is our final response to your email dated June 15, 2020 attaching a Freedom of Information Act (FOIA) request.

Specifically, your request seeks:

(a) All documents, records, communications, and other tangible evidence supporting Gen. Demers's claims to 60 minutes above, i.e., about Russian involvement in obtaining the DNC emails in 2016.

(b) All documents, records, communications, and other tangible evidence relied on by Gen. Demers, Adam Hickey, Sean Newell, and Heather Alpino in support of their conclusions that Russians were responsible for obtaining the DNC emails in 2016.

(c) All documents, records, communications, and other tangible evidence in the possession or control of the National Security Division concerning Seth Conrad Rich and/or Aaron Nathan Rich.

(d) All documents, records, communications, and other tangible evidence in the possession or control of the National Security Division concerning other entities or individuals who may have played a role in stealing, hacking, leaking or improperly obtaining the DNC emails in 2016.

(e) All documents, records, communications, and other tangible evidence in the possession or control of the National Security Division indicating whether the DNC emails were hacked externally, leaked from a source inside the DNC, or otherwise transmitted to third parties such as Wikileaks. If there was one or more than one instance of hacking, leaking, or other unauthorized transmission of DNC emails in 2016, please provide details for each such incident, e.g., the dates, persons and entities involved, the data that was hacked, leaked, or otherwise transmitted, and the means by which it was hacked, leaked, or transmitted.

(f) All documents, records, communications, and other tangible evidence in the possession or control of the National Security Division or the FBI regarding whether Debbie Wasserman-Shultz or any other member of Congress was blackmailed or extorted, whether directly or indirectly, as a result of information procured by any of the following: Imran Awan, Abid Awan, Jamal Awan, Hina Alvi, Rao Abbas, or anyone affiliated with the government of Pakistan.

We have conducted a search and located records that are responsive to your request. We are

withholding in part, one record pursuant to the following FOIA exemption set forth in 5 U.S.C. 552(b):

(6) Which permits the withholding of personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.

Please note that three discrete categories of law enforcement and national security records are excluded from the requirements of FOIA. *See* 5 U.S.C. § 552(c). This response is limited to those records that are subject to the requirements of FOIA. This is a standard notification that is given to all our requesters and should not be taken as an indication that excluded records do, or do not, exist. Additionally, NSD maintains investigative and prosecutorial files pertaining to subjects of NSD investigations. We do not routinely search these records in response to requests regarding NSD investigations in cases where the confirmation or denial of the existence of responsive records would, in and of itself, reveal information which would constitute a clearly unwarranted invasion of personal privacy of third parties or would reasonably be expected to interfere with enforcement proceedings. Accordingly, we can neither confirm nor deny the existence of records that may be potentially responsive to your request pursuant to 5 U.S.C. 552(b)(6) and/or (7)(A) and/or (7)(C).

As this matter is already in litigation, we are omitting our standard appeal paragraph. If you have any questions concerning this response please contact Assistant United States Attorney, Andrea Parker of the Eastern District of Texas at (409) 839-2538.

Notwithstanding the pending litigation, you may also contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire about the FOIA mediation services they offer to try to resolve disputes between FOIA requesters and federal agencies. The contact information for OGIS is as follows: Office of Government Information Services, National Archives and Records Administration, 8601 Adelphi Road-OGIS, College Park, Maryland 20740-6001, e-mail at ogis@nara.gov; telephone at (202) 741-5770; toll free at (877) 684-6448; or facsimile at (202) 741-5769. You also have the right to seek dispute resolution services through the DOJ's FOIA Public Liaison. NSD FOIA's Public Liaison, Patricia Matthews, may be reached by telephone at (202) 233-0756.

Sincerely,



Kevin G. Tiernan
Records and FOIA

Enclosure

From: b6 (NSD)
To: b6 (NSD)
Subject: Binder for John
Date: Tuesday, October 29, 2019 11:48:00 AM
Attachments: [Morenets Indictment.pdf](#)
[khusyaynova_complaint.pdf](#)
[indictment_concord_management.pdf](#)
[Order.pdf](#)
[netyksho_et_al_indictment.pdf](#)

Hi b6,

I'm putting together a binder for John before the prep for his 60 Minutes Interview on Thursday. When you have a moment, would you mind putting the attached in a binder? I'm going to add a couple more documents, but it's going to take me some time to gather the right items (sifting through some voluminous reports).

- Order
- Netykscho Indictment
- Khusyaynova Complaint
- Concord Management Indictment
- Morenets Indictment

Thank you!

b6

Counsel to the Assistant Attorney General
National Security Division

(U) b6

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA

v.

Criminal No.

18-263

ALEKSEI SERGEYEVICH MORENETS
EVGENII MIKHAYLOVICH SEREBRIAKOV
IVAN SERGEYEVICH YERMAKOV
ARTEM ANDREYEVICH MALYSHEV
DMITRIY SERGEYEVICH BADIN
OLEG MIKHAYLOVICH SOTNIKOV
ALEXEY VALEREVICH MININ

Defendants.

18 U.S.C. §§ 371, 1030(a)(2)(C),
1030(a)(5)(A)
(Conspiracy)
18 U.S.C. § 1349 and § 3559(g)(1)
(Conspiracy to Commit Wire Fraud)
18 U.S.C. § 1343 (Wire Fraud)
18 U.S.C. § 1028A
(Aggravated Identity Theft)
18 U.S.C. § 1956(h)
(Conspiracy to Launder Money)

[UNDER SEAL]

INDICTMENT

COUNT ONE
(Conspiracy)

The grand jury charges:

1. At all times relevant to the indictment, from at least 2014 up to and including May 2018, the Russian Federation (Russia) operated a military intelligence agency called the Main Intelligence Directorate of the General Staff (GRU). The GRU was headquartered in Moscow, Russia, and was comprised of multiple units, including Units 26165 and 74455. Military Unit 26165, also known as the “GRU 85 Main Special Service Center,” was located at 20 Komsomolskiy Prospekt, Moscow, Russia. Military Unit 74455 was located at 22 Kirova Street, Khimki, Moscow, Russia.

FILED
OCT 03 2018
CLERK U.S. DISTRICT COURT
WEST. DIST. OF PENNSYLVANIA

2. During the charged timeframe, members of the GRU conducted persistent and sophisticated criminal cyber intrusions by hacking into the computers of victims that included U.S. persons, corporate entities, international organizations and their respective employees. These victims were located around the world, including in the Western District of Pennsylvania, and were targeted by the GRU for their strategic interest to the Russian government.

3. Specifically, defendants ALEKSEI SERGEYEVICH MORENETS, EVGENII MIKHAYLOVICH SEREBRIAKOV, IVAN SERGEYEVICH YERMAKOV, ARTEM ANDREYEVICH MALYSHEV, DMITRIY SERGEYEVICH BADIN, OLEG MIKHAYLOVICH SOTNIKOV and ALEXEY VALEREVICH MININ were GRU officers who knowingly and intentionally conspired with each other, and with persons known and unknown to the grand jury, (collectively, the conspirators) to gain unauthorized access (to “hack”) into victim computers and steal private or otherwise sensitive information, in violation of United States laws. In many instances, the stolen information was publicized by the GRU as part of a related “influence and disinformation” campaign designed to undermine the legitimate interests of the victims, further Russian interests, retaliate against Russia’s detractors and sway public opinion in Russia’s favor.

THE VICTIMS

4. Among those victims targeted by the GRU were U.S. and international anti-doping agencies, sporting federations, anti-doping officials, other sports-related organizations and nearly 250 athletes from approximately 30 countries. The victims included, among others, the following:

- the U.S. Anti-Doping Agency (USADA), a U.S. based agency, headquartered in Colorado Springs, Colorado;

- the World Anti-Doping Agency (WADA), an international agency, headquartered in Montreal, Canada;
- the Canadian Centre for Ethics in Sport (CCES), a Canadian-based anti-doping agency, headquartered in Ottawa, Canada;
- the International Association of Athletics Federations (IAAF), an international sports gaming body, headquartered in Monaco;
- The Court of Arbitration for Sport (TAS/CAS), headquartered in Lausanne, Switzerland; and,
- the Fédération Internationale de Football Association (FIFA), an international governing body for football, headquartered in Zurich, Switzerland.

5. These victims were targeted by the GRU for their role in the investigation or public condemnation of Russia's state-sponsored athlete doping program and their public support of, or involvement in, a ban on Russian athletes in worldwide athletic competitions (including the 2016 Summer Olympics and Paralympics in Rio de Janeiro, Brazil). The GRU also targeted the victims to steal athletes' medical records which were then publicized as part of an influence and disinformation campaign.

6. In addition to anti-doping agencies, the GRU targeted other victims of potential benefit to Russian interests, including:

- Westinghouse Electric Corporation (WEC), a nuclear energy company headquartered in the Western District of Pennsylvania;
- the Organisation for the Prohibition of Chemical Weapons (OPCW), an organization headquartered in The Hague, Netherlands, investigating the use of

chemical weapons in Syria and the March 2018 poisoning of a former GRU officer and others in the United Kingdom with a chemical nerve agent; and,

- the Spiez Swiss Chemical Laboratory located in Spiez, Switzerland, an accredited laboratory of the OPCW that analyzed the chemical agent connected to the poisonings of a former GRU officer and others in the United Kingdom.

Cyber Intrusions and Related Influence and Disinformation Campaigns

7. The cyber intrusions conducted by the GRU involved sophisticated, persistent and unauthorized access into the victims' computer networks for the purpose of stealing private or otherwise sensitive information.

8. The hacking was often conducted remotely, from Russia. If the remote hack was unsuccessful or if it did not provide the conspirators with sufficient access to victims' networks, "on-site" or "close access" hacking operations were conducted by the conspirators. On-site operations involved trained GRU hackers with sophisticated hacking equipment traveling to victims' locations around the world. These on-site operations often involved targeting the computer networks used by victims organizations or their personnel through Wi-Fi connections, such as hotel Wi-Fi networks, in an effort to gain unauthorized access to the victims' computer networks.

9. Defendants MORENETS and SEREBRIAKOV were two such on-site GRU hackers who traveled to foreign countries with other conspirators, in some instances using Russian government issued diplomatic passports to conduct on-site operations. (See Exhibit A).

10. The intrusions were typically conducted by the conspirators for the purpose of stealing private or otherwise sensitive information.

11. The conspirators thereafter publicly released select items of stolen information under the false auspices of a hacktivist group calling itself the “Fancy Bears’ Hack Team.” The conspirators publicly disseminated the stolen information using online accounts and other infrastructure. These accounts and associated infrastructure were acquired and maintained by GRU Unit 74455.

12. Among the goals of the conspiracy was to publicize stolen information to conduct an influence and disinformation campaign designed to:

- (i) undermine, retaliate against and otherwise delegitimize the efforts of international anti-doping organizations and officials who had publicly exposed Russian government-sponsored doping by Russian athletes;
- (ii) pose as the “Fancy Bears’ Hack Team,” publicize and expose individual sensitive medical information and drug testing results of athletes;
- (iii) damage the reputations of clean athletes from various countries by falsely claiming that such athletes were using banned or performance-enhancing drugs.

THE DEFENDANTS

13. During the timeframe of the conspiracy, ALEKSEI SERGEYEVICH MORENETS (Моренец Алексей Сергеевич) served as a Russian military intelligence officer assigned to Unit 26165. MORENETS was a member of a Unit 26165 team that traveled with technical equipment to locations around the world to conduct on-site hacking operations to target and maintain persistent access to Wi-Fi networks used by victim organizations and personnel. As early as July 2016 and continuing through September 2016, MORENETS targeted U.S. and international anti-doping agencies and sporting federations in Rio de Janeiro, Brazil (July and August 2016, prior to

and during the 2016 Summer Olympics) and Lausanne, Switzerland (September 2016). MORENETS did so by compromising Wi-Fi networks used by anti-doping personnel with access to the networks of USADA, WADA and CCES. Additionally, in April 2018, MORENETS was encountered while conducting an on-site hacking operation targeting the Organisation for the Prohibition of Chemical Weapons (OPCW) in The Hague, Netherlands, and intended to thereafter target the Spiez Swiss Chemical Laboratory in Switzerland.

14. During the timeframe of the conspiracy, EVGENII MIKHAYLOVICH SEREBRIAKOV (Серебряков Евгений Михайлович) served as a Deputy Head of Directorate, Section Chief, assigned to Unit 26165. SEREBRIAKOV was another member of a Unit 26165 team that participated in the on-site hacking operations in Rio de Janeiro, Brazil (August 2016), and Lausanne, Switzerland (September 2016), that targeted USADA, WADA and CCES. In April 2018, SEREBRIAKOV targeted the OPCW in The Hague, Netherlands, and intended to thereafter target the Spiez Swiss Chemical Laboratory in Switzerland.

15. During the timeframe of the conspiracy, IVAN SERGEYEVICH YERMAKOV (Ермаков Иван Сергеевич) served as a Russian military intelligence officer in the GRU assigned to Unit 26165. YERMAKOV conducted technical and online reconnaissance of victim organizations, their employees and their computer networks and thereafter sent spearphishing emails using fictitious personas and proxy servers in an attempt to obscure his identity and GRU affiliation. YERMAKOV also participated in, and provided remote support to, MORENETS' and SEREBRIAKOV's on-site hacking operations, all on behalf of Unit 26165. As early as November 2014 and continuing through at least August 2016, YERMAKOV and his co-conspirators targeted Westinghouse Electric Corporation (WEC) and its employees, in the Western District of

Pennsylvania, WADA and USADA. YERMAKOV is a charged defendant in federal indictment number CR 18-215 in the District of Columbia.

16. During the timeframe of the conspiracy, ARTEM ANDREYEVICH MALYSHEV (Мальшев Артём Андреевич) served as a Senior Lieutenant assigned to Unit 26165. In 2016, MALYSHEV monitored X-Agent malware (a/k/a “Chopstick”) implanted on victim networks and utilized online fictitious personas to conduct technical and online reconnaissance of victim organizations and to send spearphishing emails, all on behalf of Unit 26165. As early as July 2016 and continuing through at least August 2016, MALYSHEV participated in intrusion activities targeting WADA. MALYSHEV is a charged defendant in federal indictment number CR 18-215 in the District of Columbia.

17. During the timeframe of the conspiracy, DMITRIY SERGEYEVICH BADIN (Бадин Дмитрий Сергеевич) was an “Assistant Head of Department” assigned to Unit 26165. In his supervisory role, BADIN oversaw the criminal activities of conspirators as they engaged in computer intrusions and stole credentials, medical records and other data. BADIN also compiled and used malware and other tools to aid in the compromise of victim networks by the conspirators, including the CCES network in September and October 2016. BADIN is a charged defendant in federal indictment number CR 18-215 in the District of Columbia. (Images of defendants YERMAKOV, MALYSHEV and BADIN are attached as Exhibit B).

18. During the timeframe of the conspiracy, OLEG MIKHAYLOVICH SOTNIKOV (Олег Михайлович Сотников) served as a Russian military intelligence officer. SOTNIKOV provided support to his conspirators during their targeting of the OPCW in The Hague, Netherlands, and intended to thereafter target the Spiez Swiss Chemical Laboratory in Switzerland.

19. During the time period of the conspiracy, ALEXEY VALEREVICH MININ (Алексей Валерьевич Минин) served as a Russian military intelligence officer. MININ provided support to MORENETS and SEREBRIAKOV during their targeting of the OPCW in The Hague, Netherlands, and intended to thereafter target the Spiez Swiss Chemical Laboratory in Switzerland. (See Exhibit A, images of SOTNIKOV and MININ).

MANNER AND MEANS OF THE CONSPIRACY

20. The members of the conspiracy, who are both known and unknown to the grand jury, used the following manner and means to accomplish their objectives, which included gaining unauthorized access to computers at entities of interest to the Russian government, including Westinghouse Electric Company (WEC), the U.S. Anti-Doping Agency (USADA), the World Anti-Doping Agency (WADA), the Canadian Centre for Ethics in Sport (CCES), Court of Arbitration for Sport (TAS/CAS), the International Association of Athletics Federations (IAAF), the Fédération Internationale de Football Association (FIFA), and the Organisation for the Prohibition of Chemical Weapons (OPCW). Conspirators further used that unauthorized access to steal information and, in some instances, publicized the stolen materials to engage in influence and disinformation operations to advance the interests of the Russian government.

21. In order to avoid detection by law enforcement, security researchers and victims, and to mask their GRU affiliation and location in Russia, the conspirators used a variety of fictitious names and personas, as well as online infrastructure, including servers, domains, cryptocurrency, email accounts, social media accounts and other online services provided by companies in the United States and elsewhere. The conspirators used this infrastructure for a wide range of conduct in furtherance of the conspiracy: to communicate, research and probe victims and

their computer networks; to send spearphishing emails; to mimic legitimate domains and websites; to store and distribute additional malware; to manage malware; to transfer stolen data; to publicly release stolen information; to draw public and media attention to such stolen information; and, to negatively influence the perception of such stolen information and the victims. Conspirators used common infrastructure to target multiple victim organizations and individuals. For example, the conspirators utilized approximately 38 common IP addresses to conduct the intrusion activities at both WADA and USADA, and much of the stolen information from all of the anti-doping-related victims was posted and disseminated through the social media accounts or website of the Fancy Bears' Hack Team, fancybear.net and fancybear.org.

22. In those instances where conspirators purchased hacking infrastructure, payments were made using a complex web of transactions involving operational accounts in fictitious names and typically utilized cryptocurrencies, such as Bitcoin, to further mask their identities and conduct.

23. The conspirators typically initiated their hacking activities by researching the victim organizations, including their computer networks and employees. This research provided technical and biographical information that the conspirators could exploit in subsequent intrusion activities.

24. The conspirators also registered domain names for use in their hacking activities. Examples include "westinqhousenuclear.com" (deliberately substituting a "q" for a "g,"), "wada.awa.org" and "wada.arna.org" (WADA's legitimate domain was "wada.ama.org"). These domains were intended to mimic or "spoof" those of legitimate websites that victims were familiar with, including webmail login pages, VPN login screens or password reset pages.

25. Frequently, the conspirators crafted email messages known as “spearphishing,” designed to trick unwitting recipients into giving the conspirators access to their computers and account credentials (e.g., a username and password). Spearphishing messages were composed to resemble emails from trustworthy senders, such as email providers or colleagues, and requested the recipients to click on hyperlinks in the messages. Such hyperlinks would direct recipients to spoofed websites which prompted the recipients to enter their login and password and enabled the capture of their credentials. In many cases, the hyperlinks were created using an online service (e.g., Bit.ly) that abbreviated lengthy website addresses (referred to as a “URL-shortening service”). In other cases, the hyperlinks were domains that the conspirators registered for a fee with online providers, such as “wada.awa.org,” and “wada.arna.org.”

26. When the conspirators’ remote hacking efforts failed to capture log-in credentials, or if those accounts that were successfully compromised did not have the necessary access privileges for the sought-after information, teams of GRU intelligence officers traveled to locations around the world where targets were physically located. Using specialized equipment, and with the remote support of conspirators in Russia, these on-site teams hacked into Wi-Fi networks used by victim organizations or their personnel, including hotel Wi-Fi networks. After a successful hacking operation, the on-site, or close access, team transferred such access to conspirators in Russia.

27. The conspirators developed and utilized malware and hacking tools, including “Gamefish,” “X-agent” (a/k/a “Chopstick”), “X-tunnel,” “Remcomsvc,” and “Responder.exe,” in order to hack and compromise victim computers and networks, to maintain command and control over such networks, and to steal network credentials and other sensitive and private data.

28. After hacking into victim computers, remotely or aided by the on-site teams, the conspirators performed a variety of functions designed to identify, collect, package and steal targeted data from the victims' computers. In instances where the hacking was part of an influence or disinformation operation, conspirators publicly posted and disseminated such information, including victims' personal email communications and individual health and medical information. In some instances, such information was modified from its original form. Thereafter, the conspirators would actively solicit and promote media coverage so the stolen information would receive international attention. This was done to further a narrative favorable to the Russian government and in order to amplify its impact.

COMPUTER INTRUSIONS and OTHER OVERT ACTS

Westinghouse Electric Company (WEC)

29. At all times during the conspiracy, WEC was a U.S.-based nuclear power developer, with its headquarters outside of Pittsburgh, Pennsylvania, that provided fuel, services and plant design to international customers in the commercial nuclear industry. All of WEC's internet traffic is routed through servers located in the Western District of Pennsylvania. The company's power plant designs are the basis for approximately half of the world's currently operating nuclear power plants. Since 2008, WEC has supplied Ukraine with increasing amounts of nuclear fuel.

30. As early as November 20, 2014, IVAN SERGEYEVICH YERMAKOV performed technical reconnaissance of WEC, WEC-related IP addresses, network ports and associated domains. On December 8, 9, and 22, 2014, YERMAKOV's reconnaissance included research on WEC, its employees, and their background in nuclear energy research and development.

31. On December 10, 2014, YERMAKOV and his co-conspirators registered a fake domain and website, “https://webmail.westinghousenuclear.com” to mimic a legitimate WEC domain. Spearphishing emails were sent to at least five WEC employees, designed to appear as routine emails from the Westinghouse.com Microsoft Exchange Server. Upon clicking an enclosed link, users were directed to the spoofed domain where their login credentials were stolen and saved. Once stolen credentials were determined to be authentic by the conspirators, victims were then re-routed to the original, legitimate WEC network so that they were unaware that the theft of their passwords had occurred.

32. Following the targeting of WEC corporate accounts, on December 24, 2014, January 15, 2015, January 17, 2015 and November 18, 2015, using Bit.ly accounts, YERMAKOV and conspirators sent spearphishing emails to the personal email accounts of four WEC employees who resided near Pittsburgh, Pennsylvania. The users of two of the accounts clicked on the malicious link which would have enabled the theft of the login credentials to their personal email accounts. These employees worked in the nuclear energy field and were involved in advanced nuclear reactor development and new reactor technology.

World Anti-Doping Agency (WADA)

33. WADA was established under the initiative of the International Olympic Committee (IOC) in 1999 as an international independent agency, which is composed of and funded equally by the sports movement and governments of the world. WADA, which is headquartered in Montreal, Canada, administers the World Anti-Doping Code – the document harmonizing anti-doping policies in all sports and all countries - and coordinates anti-doping activities internationally through its central drug testing clearinghouse, the Anti-Doping

Administration and Management System (ADAMS) database. The ADAMS database contains laboratory results of drug tests and location information for nearly 30,000 athletes in addition to records related to the granting or denial of therapeutic use exemptions (TUEs) for otherwise prohibited substances. Athletes whose medical information resides in the ADAMS database reside throughout the world, including in the Western District of Pennsylvania.

34. In 2014, a German documentary titled, “Top Secret Doping: How Russia Makes its Winners,” aired interviews of husband and wife Russian whistleblowers who admitted to participation in the Russian state-sponsored doping program as an anti-doping official and athlete, respectively. Shortly thereafter, WADA launched an Independent Commission (IC) to investigate the validity of the allegations. In a November 2015 report, the WADA IC released its findings, namely, it “confirmed the existence of widespread cheating through the use of doping substances and methods to ensure, or enhance the likelihood of, victory for [Russian] athletes and teams.” The IC made “specific findings” regarding the involvement of the Russian Federal Security Service (FSB) in Russia’s efforts to evade anti-doping procedures and protections.

35. In May 2016, a prominent television newsmagazine and newspaper each published stories regarding allegations from the husband and wife whistleblowers, as well as a new Russian whistleblower who had previously managed Russia’s anti-doping laboratory. The whistleblowers all alleged a Russian state-sponsored doping effort at the 2014 Sochi Winter Olympics. In response, WADA named an “independent person” (IP) to investigate their allegations.

36. On July 18, 2016, the WADA-appointed IP published his first report, the “McLaren Report,” regarding Russia’s systematic state-sponsored subversion of the drug testing processes prior to, during and subsequent to the 2014 Sochi Winter Olympics. WADA’s Executive

Committee issued a statement accompanying this report, which recommended that the IOC and the International Paralympic Committee (IPC) “decline entries for Rio [Olympics and Paralympics] 2016, of all athletes submitted by the Russian Olympic Committee (ROC) and the Russian Paralympic Committee.” Beginning that same day, multiple IP addresses were used to scan WADA’s network for vulnerabilities or potential access points.

37. On July 24, 2016, the IOC Executive Board announced a “preliminary decision” (later affirmed by the broader IOC) that, as a result of the WADA IP’s report, individual sporting federations could exclude Russian athletes from the 2016 Rio Summer Olympics, with each positive decision having to be approved by an arbitrator from the international Court of Arbitration for Sport (TAS/CAS). Ultimately, 111 Russian athletes were barred from participation in the Olympics. The IPC issued a blanket ban of Russian athletes for the 2016 Rio Summer Paralympics.

38. The next day, on July 25, 2016, conspirators launched a Distributed Denial-of-Service (DDoS) attack against, and vulnerability scan, of WADA’s official website: wada-ama.org.

Compromise of WADA’s Computer Networks

39. On August 2, 2016, conspirators used multiple IP address to connect to or scan WADA’s network. Such activity continued on August 4, 5, 8 and 9, 2016.

40. Also on August 2, 2016, defendant YERMAKOV researched WADA and password recovery requirements for WADA’s ADAM’s database.

41. On August 3, 2016, conspirators registered the domain “wada.awa.org” using an email account and a fictitious name. This registered domain spoofed, or falsely mimicked, WADA’s legitimate domain: wada-ama.org.

42. On August 3 and 4, 2016, defendant YERMAKOV researched WADA and ADAMS, as well as exploits and other hacking techniques.

43. On August 4, 2016, conspirators, including defendant MALYSHEV, sent spearphishing emails to eleven WADA employees, appearing to be from the WADA Chief Technology Officer, which prompted the employees to click on the link to authenticate their WADA email accounts. In fact, the link was designed to steal WADA employee login credentials. Approximately four WADA employees clicked on the malicious link which enabled conspirators to steal their login account credentials, which were later used to access their WADA accounts.

44. On August 5, 2016, defendant YERMAKOV conducted research regarding WADA, the WADA-appointed IP, the McLaren Report and CISCO firewalls. This included research of a specific WADA employee, including his or her LinkedIn profile. Minutes later, conspirators created a link embedding that employee’s email address using the URL-shortening service Bit.ly, and a corresponding spearphishing email was sent to the victim’s email account. The employee clicked on the malicious link which was designed to allow defendant YERMAKOV and the conspirators to harvest his or her log-in credentials and gain access to his or her emails. Over the course of the conspirators’ targeting of WADA, this Bit.ly account created links for the personal email accounts of at least four WADA employees.

45. On August 8, 2016, conspirators registered the domain “wada-arna.org” using an email account and a fictitious name. This registered domain spoofed, or falsely mimicked, WADA’s legitimate domain: wada-ama.org.

46. That same day, and again on August 9, 2016, defendant YERMAKOV continued research targeting WADA employees. He also prepared to send spearphishing emails, by composing English-language draft emails and by researching information regarding CISCO security updates, CISCO access and privilege escalation. On August 9, 2016, defendant MALYSHEV also prepared to send spearphishing emails by conducting research and reviewing a draft spearphishing email.

47. On August 9, 2016, defendants YERMAKOV and MALYSHEV sent spearphishing emails written to appear as if they were from a WADA IT Manager to WADA employees prompting them to click on a link to “update their Cisco client.” At least one WADA employee clicked on the link and entered his or her login credentials.

Compromise of WADA’s
Computer Networks Through On-Site Operations

48. Conspirators made two operational trips to Rio de Janeiro, the site of the 2016 Summer Olympics and Paralympics, to conduct hacking operations targeting and maintaining persistent access to Wi-Fi networks used by anti-doping officials. First, from July 10 through July 19, 2016, prior to the Olympics, defendant MORENETS traveled to Rio. Second, from August 13, 2016 to August 19, 2016, during the Olympics, defendants MORENETS and SEREBRIAKOV traveled together to Rio.

49. During defendants MORENETS’ and SEREBRIAKOV’s second trip to Rio, defendant YERMAKOV provided remote support to their close access operation. For example,

on August 13 and 14, 2016, defendant YERMAKOV conducted research concerning an identified hotel chain that hosted Olympics officials, including IOC, TAS/CAS, WADA and USADA officials. Within minutes, defendant YERMAKOV also researched the routers used by some of those hotels for Wi-Fi access and methods of exploiting those routers, including through “brute force” password cracking.

50. On August 19, 2016, approximately 15 hours before defendants MORENETS’ and SEREBRIAKOV’s departure from Rio, an identified IOC anti-doping official used his or her administrator credentials to log into WADA’s ADAMS database from a Brazilian IP address. The conspirators captured that IOC official’s username and password and thereafter used them, and another set of ADAMS credentials belonging to the same official that was created specifically for anti-doping officials at the Rio Olympic games, to gain unauthorized access to the ADAMS database and medical and anti-doping-related information available to those accounts. The broader ADAMS database was not compromised in the attack. The conspirators conducted large-scale exports of data from WADA’s networks on August 29, 2016 and September 6, 2016.

Tribunal Arbitral du Sport/Court of Arbitration for Sport (TAS/CAS)

51. TAS/CAS is an independent institution based in Lausanne, Switzerland, which resolves sports-related legal disputes through arbitration. In this capacity, TAS/CAS was involved in the Russian doping scandal, including a July 21, 2016 decision to uphold the suspension by IAAF of the All-Russia Athletics Federation and the July 24, 2016 decision by the IOC that individual sporting confederations could ban Russian athletes from the Rio Olympics, with the approval of a TAS/CAS arbitrator. On July 26, 2016, TAS/CAS established an *ad hoc* tribunal to

resolve disputes at the Rio Olympics, which was located at a Rio hotel operated by the hotel chain described herein as having been targeted by defendant YERMAKOV.

52. On August 8, 2016, the conspirators used the same email account and fictitious name that was used to register the spoofed “wada-arna.org” domain to register a second domain “tas-cass.org.” The registered domain falsely mimicked TAS/CAS’ legitimate domain: tas-cas.org.

53. One day later, on August 9, 2016, defendants MALYSHEV and YERMAKOV conducted online reconnaissance efforts targeting TAS/CAS email accounts and made other preparations for sending spearphishing emails.

U.S. Anti-Doping Agency (USADA)

54. USADA is the national anti-doping organization in the United States for Olympic and Paralympic Sports. USADA implements a national anti-doping program that includes athlete testing and also oversees therapeutic use exemptions (TUEs) for prohibited substances, consistent with the World Anti-Doping Code and in coordination with WADA and the IOC. Like WADA, USADA maintains thousands of sensitive, confidential records regarding the location of United States athletes, their drug testing history and results and TUEs. USADA is headquartered in Colorado Springs, Colorado.

55. During the timeframe of the conspiracy, USADA leadership was publicly outspoken regarding its concern about state-sanctioned doping among Russian athletes and advocated for a ban of Russian athletes from the 2016 Rio Olympics. This included cooperative efforts with CCES and other national anti-doping agencies in July 2016 to make a concerted push for a ban upon the anticipated release of the WADA McLaren Report. USADA was also a vocal

critic of the IOC's July 24, 2016 decision not to institute a full ban on Russian athletes participating in the 2016 Rio Olympics, releasing a statement that, "the decision regarding Russian participation and the confusing mess left in its wake is a significant blow to the rights of clean athletes."

56. On August 2, 2016, defendant YERMAKOV conducted research of USADA.

57. On August 14, 2016, conspirators began efforts to compromise USADA's network, including through "SQL injection" attacks against USADA's "ufcathlete.usada.org" website from multiple IP addresses (SQL injection attacks are a hacking technique that involved typing commands in the website's fields in order to tamper with, steal or gain unauthorized access to a database). USADA also administers the anti-doping program for the Ultimate Fighting Championship (UFC) and specifically maintains a Russian language option for its UFC athletes. These attacks, which consisted of 24,227 SQL injection attempts from 62 different sources, continued intermittently until August 18, 2016, and used some of the same infrastructure from similar attacks against WADA during the same time frame. The SQL injection attacks, as captured on USADA logs, show that the hackers attempted to use the "change language" function to switch from English to Russian.

58. In late August 2016, a senior USADA anti-doping official traveled to Rio de Janeiro, Brazil for the Olympics and Paralympic games. At that time, the USADA official served on the IPC which had unanimously suspended Russia from official participation in the 2016 Rio Paralympics. A number of anti-doping officials stayed at a Rio hotel operated by the hotel chain described herein as having been targeted by defendant YERMAKOV. Throughout his or her stay, the USADA official used Wi-Fi at his or her hotel and other Wi-Fi access points in Rio to remotely access USADA's computer systems and conduct official business via his or her portable electronic

devices.

59. On August 19 and 25, 2016, conspirators sent spearphishing emails to the personal account of an officer serving on the USADA Board of Directors. The emails contained a malicious link that was created by the same Bit.ly account used to send spearphishing emails to WADA employees in August 2016.

60. On September 6, 2016, while the USADA official was still in Rio, conspirators successfully compromised the credentials for his or her USADA VPN account and Office 365 Exchange mailbox, the latter of which contained all of his or her emails. At that time, the USADA official's account contained over 90,000 messages and an estimated 10 gigabytes of data, which included summaries of athlete test results and prescribed medications.

61. The conspirators subsequently attempted to use the USADA official's credentials to gain unauthorized access to 33 separate USADA systems between September 7 and 14, 2016. These attempts were ultimately unsuccessful.

Canadian Centre for Ethics in Sport (CCES)

62. CCES is the national anti-doping organization for Canada and oversees the implementation and management of Canada's Anti-Doping Program. During the timeframe of the conspiracy, CCES coordinated drug testing and analysis, assured adherence to the World Anti-Doping Code and considered exemptions for athletes with medical conditions. The headquarters for CCES are in Ottawa, Canada.

63. During the conspiracy, CCES leadership spoke out publicly against Russia's state-sponsored doping program and joined with USADA in support of a ban for the Rio Olympics and beyond. On September 19, 2016, CCES issued a media release condemning the hacking of WADA

and the athlete information in the ADAMS database, as well as the public posting of such information.

64. In mid-September 2016, a senior CCES official traveled to Lausanne, Switzerland for a WADA-hosted anti-doping conference. Conference proceedings and lodging were hosted at a specific hotel in Lausanne (Lausanne Hotel 1), which offered Wi-Fi for its guests. During this trip, the CCES official traveled with a laptop computer, stayed at Lausanne Hotel 1 and used the hotel Wi-Fi connection to access the internet and conduct official business.

65. On September 18, 2016, defendants MORENETS and SEREBRIAKOV traveled to Lausanne, Switzerland, with defendant SEREBRIAKOV staying in Lausanne Hotel 1, and defendant MORENETS staying in a second hotel in close proximity (Lausanne Hotel 2), which was also hosting anti-doping officials as guests. Both reservations were for four nights. Defendants MORENETS and SEREBRIAKOV were at the time in possession of equipment used for on-site or close access Wi-Fi compromises.

66. On September 19, 2016, while the CCES official was staying at Lausanne Hotel 1 and connected to the hotel's Wi-Fi network, defendants MORENETS and SEREBRIAKOV, together with co-conspirators, compromised the hotel Wi-Fi network to gain unauthorized access to the CCES official's laptop. Using that access, the conspirators accessed the CCES official's emails and placed, or attempted to place, malware, namely Gamefish, X-agent, X-Tunnel, Remcomsvc, and Responder.exe, onto the laptop.

67. On September 20, 2016, while at Lausanne Hotel 1, the CCES official happened to check the "Sent items" email folder on his laptop. In the folder, he or she found a message to the Chief Medical Officer of another international sporting organization that he or she had neither

composed nor sent. The message contained several blatant typographical errors and inaccurately attempted to mimic the cell phone signature line of the CCES officer: "Sent from my SamsunCopenhagen." The message also contained what appeared to be an embedded malicious link.

68. Starting on September 20, 2016, the conspirators, using the CCES official's credentials, moved laterally from the CCES official's laptop to CCES' computer network in Canada. The conspirators maintained access to, and installed tools and malware Gamefish, X-agent, and Remcomsvc, on the CCES network until at least October 24, 2016, when CCES took its network offline.

69. Forensic evidence obtained from CCES revealed that the conspirators had used a file named "vsc.exe," which was a tool used to extract hashed passwords from a victim computer network. Analysis of the metadata of this tool revealed that it had been compiled by defendant DMITRIY SERGEYEVICH BADIN.

International Association of Athletics Federations (IAAF)

70. The IAAF is an international sports federation that governs track-and-field competitions and related standardized technical equipment and official world records. During the timeframe of the conspiracy, the IAAF maintained an anti-doping department and staff, which was transitioned into a newly-formed IAAF "Athletics Integrity Unit" (AIU) in April 2017. Even before the establishment of the AIU, IAAF's anti-doping staff were responsible for all aspects of the anti-doping program for international-level athletes, including education, testing, intelligence gathering, investigations, results management, prosecutions and appeals. The IAAF is headquartered in the Principality of Monaco.

71. On November 13, 2015, shortly after WADA released its first report, the Council of the IAAF provisionally suspended the membership of the All-Russia Athletics Federation (ARAF) in response to allegations of Russian state-sponsored doping allegations. On July 21, 2016, TAS/CAS upheld ARAF's suspension and Russian track-and-field athletes were barred from the 2016 Rio Olympics. Since that time, IAAF has continued the suspension, in part due to the refusal by ARAF and Russian sporting officials to acknowledge the McLaren Report's findings.

72. From January 19 to 24, 2017, three weeks before the IAAF was to release a recommendation regarding ARAF's reinstatement, the conspirators compromised the computers of at least four IAAF officials, including the head of IAAF's anti-doping department. Specifically, through malware placed on the IAAF network, including X-agent, the conspirators were able to review keylogger results, monitor Skype communications and access file directories. Prior to these specific events, the command and control infrastructure for the IAAF X-agent malware was managed from an IP address frequently used by MALYSHEV.

Fédération Internationale de Football Association (FIFA)

73. FIFA is an international sports federation that governs football (soccer). During the timeframe of the conspiracy, FIFA maintained a Medical and Anti-Doping Unit that directly administered the anti-doping programs for all FIFA competitions through a worldwide network of doping control officers. FIFA is headquartered in Zurich, Switzerland.

74. A second, more detailed report released by WADA on December 9, 2016 (the "Second McLaren Report") included evidence that Russian football players may have been involved in the state-sponsored doping scandal. As a result, FIFA announced an investigation.

75. From at least December 6, 2016 to January 2, 2017, the conspirators compromised a computer belonging to the head of FIFA's Medical and Anti-Doping Unit. Specifically, through malware placed on the computer, including X-agent, the conspirators downloaded more than 100 documents related to the First and Second McLaren Reports, including supporting evidence, FIFA's anti-doping policy and strategy, lab results, medical reports, contracts with doctors and medical testing labs, information about medical testing procedures and TUEs. Prior to these specific events, the command and control infrastructure for the X-agent malware was managed from an IP address frequently used by defendant MALYSHEV.

Influence and Disinformation Operations Using Stolen Information

76. Beginning on or about September 1, 2016, and continuing in separate installments through May 2018, the conspirators, falsely claiming to be the hacktivist group Fancy Bears' Hack Team, used online accounts and other infrastructure procured and managed, at least in part, by conspirators in GRU Unit 74455 to release data stolen from WADA, USADA, CCES, TAS/CAS, IAAF, and FIFA, as well as data that appeared to be stolen from 35 other anti-doping agencies or sporting organizations. Such data was available to and viewed by residents in the Western District of Pennsylvania.

The Public Release of Stolen Information

77. The domains fancybear.org and fancybear.net were registered on September 1, 2016. On September 12, 2016, data stolen from WADA and its ADAMS database by conspirators first appeared on fancybear.net, including medical information for individual athletes, and private, official email communications. Although the initial disseminations focused on U.S. athletes, subsequent releases of stolen data included records of nearly 250 athletes from almost 30 countries.

These athlete records from WADA included testing history and TUEs for an athlete and resident of the Western District of Pennsylvania. Many of the WADA documents released by the conspirators did not accurately reflect their original form. On fancybear.net, individual athletes were named, categorized by nationality and sport, and identified as having such personal diagnoses as “ADD” (attention deficit disorder), “drug addiction,” “diabetes insipidus,” or “circulatory collapse.” As one example, an athlete’s stolen record was posted, listing the athlete’s date of birth, sport, nationality, the daily dose and manner of administration of a prescribed therapeutic substance, approving physician and the results of a recent (urine) drug test.

78. On or about October 6, 2016, emails and data that conspirators stole from USADA were released on fancybear.net. The records included personal medical information, such as testing histories and TUEs, for multiple athletes, including an athlete and resident of the Western District of Pennsylvania.

79. On December 13, 2016, emails and data that conspirators stole from CCES network were released on fancybear.net.

80. On or about June 22, 2017, and July 5, 2017, emails and data that conspirators stole from IAAF’s network were released on fancybear.net, including emails about doping violations of non-Russian athletes.

81. On August 28, 2017, emails and data that that conspirators stole from FIFA’s network were released on fancybear.net, including lists of players who were provided TUEs before the 2010 World Cup, a list of failed drug tests, and emails between FIFA and anti-doping officials.

The Conspirators Sustained Media Campaign

82. The conspirators released this stolen information to further one of the objectives of the conspiracy, namely to undermine and retaliate against international anti-doping officials who had exposed the Russian state-sponsored doping program at the 2014 Sochi Winter Olympics and other competitions.

83. In some instances, the Fancy Bears' Hack Team's posts and other communications parroted or supported themes that were already found in the Russian government's narrative. The following are examples of official Russian statements regarding the investigative findings:

- a. On August 2, 2016, the President of the Olympic Committee of Russia claimed that "[w]e are witnessing the direct interference of politics in sport";
- b. On August 21, 2017, the Russian Minister of Sport and the President of the Olympic Committee of Russia indicated in a joint letter to the IOC that "the problem of doping is faced not only by Russia"; and
- c. On or about February 11, 2018, the Russian Foreign Minister claimed that the accusations of state-sponsored doping were orchestrated by the United States "because they can't beat us fairly."

84. The Fancy Bears' Hack Team, on fancybear.net, made similar misleading statements, such as:

- a. "U.S. and Canada Sports Officials' Secret Plot Revealed"; and
- b. Canada and the United States "tried to further their political interests pretending to fight for clean sport";
- c. "We have proof of American athletes taking doping"; and

- d. “WADA has failed to be a viable and trusted anti-doping organization because its leadership and [national anti-doping agencies’] chiefs follow Anglo-Saxon political agenda.”

85. Between September 12, 2016 and at least January 17, 2018, the conspirators engaged in a concerted effort to draw media attention to the leaks through a proactive outreach campaign that went beyond its public social media posts. During that timeframe, the @fancybears and @fancybearHT Twitter accounts sent direct messages to the Twitter accounts of approximately 116 reporters around the world advertising the stolen information.

86. Similarly, between September 19, 2016, and July 20, 2018, the conspirators, using the Fancy Bears’ Hack Team persona, exchanged e-mails with approximately 70 reporters around the world. The only condition set forth by the conspirators in such exchanges was that reporters were required to refer to the Fancy Bears’ Hack Team by name in the story and later provide a link to the story back to the conspirators. In some cases, reporters pressed for and received promises of exclusivity in such reporting, with one such reporter attempting to make arrangements for a right of first refusal for articles on all future leaks and actively suggesting methods with which the conspiracy could search the stolen materials for documents of interest to that reporter (e.g., keywords of interest).

87. After the articles were published, conspirators used the Fancy Bears’ Hack Team social media accounts to draw attention to the articles, in an apparent attempt to amplify the exposure and effect of their message.

Organisation for the Prohibition of Chemical Weapons (OPCW)

88. The OPCW is the body that implements the Chemical Weapons Convention of

1997 and includes 193 member nations, including the United States. On April 7, 2018, the OPCW Executive Council convened at its headquarters in The Hague to discuss the use of toxic chemical weapons in Syria. Also, in April 2018, including on or about April 11 and 12, OPCW transmitted statements regarding its investigation of the March 4, 2018 poisoning of a former GRU officer and another Russian national in the United Kingdom with a chemical nerve agent.

89. On April 10, 2018, defendants ALEKSEI SERGEYEVICH MORENETS, EVGENII MIKHAYLOVICH SEREBRIAKOV, OLEG MIKHAYLOVICH SOTNIKOV and ALEXEY VALEREVICH MININ, all using Russian diplomatic passports, traveled to The Hague in the Netherlands in furtherance of another on-site operation. According to a taxi receipt found on his person, prior to his departure from Moscow on April 10, 2018, defendant MORENETS traveled by taxi from Nesvizhsky Pereulok, a street located at the rear entrance of GRU headquarters for Unit 26165, directly to Sheremetyevo Airport. (See Exhibit C).

90. Upon their arrival in the Netherlands, an identified official from the Russian Embassy escorted defendants MORENETS, SEREBRIAKOV, SOTNIKOV and MININ through customs. All four thereafter checked into a hotel situated adjacent to the OPCW headquarters in The Hague.

91. On April 11, 2018, defendants SOTNIKOV and MININ rented a car and thereafter assembled and secreted technical hacking equipment in the car's trunk. The technical equipment was capable of several techniques, including long-distance, surreptitious interception of Wi-Fi signals, as well as harvesting of Wi-Fi user credentials. The next day, all four defendants checked into a second hotel located adjacent to the OPCW headquarters in The Hague.

92. On April 13, 2018, defendants MORENETS, SEREBRIAKOV, SOTNIKOV and

MININ parked the rental car adjacent to the OPCW property, with the trunk facing the OPCW. (See Exhibit D). The hacking equipment was deployed with an antenna (covered by a jacket) aimed at the nearby headquarters of the OPCW and configured so that it could be controlled by either an attached laptop computer or through a remote 4G connection. (See Exhibit E).

93. After the GRU team activated the equipment, the Dutch defence intelligence service (Militaire Inlichtingen en Veiligheidsdienst or MIVD) disrupted the GRU team's operation. As a result, the conspirators abandoned their equipment, including defendant SEREBRIAKOV's backpack. This backpack contained additional technical equipment that the team could also use to surreptitiously intercept Wi-Fi signals and traffic, including a "Wi-Fi Pineapple." (See Exhibit F). At least one item of equipment in defendant SEREBRIAKOV's possession contained technical data indicating that it had been used to connect to hotel Wi-Fi at Lausanne Hotels 1 and 2, where defendants MORENETS and SERBRIAKOV had stayed in Switzerland on September 20-22, 2016, (the dates they conducted the Wi-Fi compromise of the senior CCES official's laptop at the same hotel), as well as multiple other international destinations, including a hotel in Kuala Lumpur, Malaysia, in December 2017. Defendant SEREBRIAKOV's equipment was also found to have contained an image that placed him at the 2016 Summer Olympics in Rio on August 14, 2016. (See Exhibit G).

94. Further data on defendant SEREBRIAKOV's equipment indicated that, on April 9, 2018, he had conducted online searches of the Spiez Swiss Chemical Laboratory, an accredited laboratory of the OPCW for conducting analysis of military chemical agents, including the chemical agent that United Kingdom authorities connected to the poisoning of the former GRU officer in the United Kingdom. Defendants MORENETS, SEREBRIAKOV, SOTNIKOV and

MININ had earlier purchased train tickets from The Hague to Bern, Switzerland, dated April 17, 2018, in order to continue their operational deployment to target the Spiez laboratory.

STATUTORY ALLEGATIONS

95. Beginning at least in or about 2014 and continuing until at least in or about May 2018, the exact dates being unknown to the Grand Jury, in the Western District of Pennsylvania and elsewhere, defendants ALEKSEI SERGEYEVICH MORENETS, EVGENII MIKHAYLOVICH SEREBRIAKOV, IVAN SERGEYEVICH YERMAKOV, ARTEM ANDREYEVICH MALYSHEV, DMITRIY SERGEYEVICH BADIN, OLEG MIKHAYLOVICH SOTNIKOV and ALEXEY VALEREVICH MININ, did knowingly and intentionally combine, conspire, confederate, and agree together, with each other and with others known and unknown to the grand jury, to commit offenses against the United States, namely:

- a. to access a computer without authorization and exceed authorized access to a computer, and to obtain thereby information from a protected computer, in furtherance of a criminal and tortious act in violation of the laws of the Commonwealth of Pennsylvania, namely, the common law tort of Invasion of Privacy, and where the value of the information did, and would if completed, exceed \$5,000, in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and 1030(c)(2)(B);
- b. to cause the transmission of a program, information, code, and command, and as a result of such conduct, to cause damage without authorization to a protected computer, and where the offense did cause and would, if completed, have caused, loss aggregating \$5,000 in value to at least one person during a one-year

period from a related course of conduct affecting a protected computer, and damage affecting at least 10 protected computers during a one-year period, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and 1030(c)(4)(B); and, All in violation of Title 18, United States Code, Section 371.

COUNT TWO
(Wire Fraud Conspiracy)

The grand jury further charges:

96. The allegations contained in Paragraphs 1 through 94 of this indictment are repeated, re-alleged, and incorporated by reference as if fully set forth herein.

THE CONSPIRACY AND ITS OBJECTS

97. From at least approximately 2014, and continuing thereafter to in and around April 2018, in the Western District of Pennsylvania and elsewhere, defendants ALEKSEI SERGEYEVICH MORENETS, EVGENII MIKHAYLOVICH SEREBRIAKOV, IVAN SERGEYEVICH YERMAKOV, ARTEM ANDREYEVICH MALYSHEV, DMITRIY SERGEYEVICH BADIN, OLEG MIKHAYLOVICH SOTNIKOV and ALEXEY VALEREVICH MININ, knowingly and willfully did conspire, combine, and agree to commit an offense against the United States, that is, wire fraud, contrary to the provisions of Title 18, United States Code, Section 1343, to wit:

the defendants, ALEKSEI SERGEYEVICH MORENETS, EVGENII MIKHAYLOVICH SEREBRIAKOV, IVAN SERGEYEVICH YERMAKOV, ARTEM ANDREYEVICH MALYSHEV, DMITRIY SERGEYEVICH BADIN, OLEG MIKHAYLOVICH SOTNIKOV and ALEXEY VALEREVICH MININ, together with conspirators, having devised and intending to devise a scheme and artifice to defraud, and to obtain property by means of false and fraudulent pretenses, representations and promises, did transmit and cause to be transmitted by means of wire

communication in interstate and foreign commerce, certain writings, signs, signals, and pictures for the purpose of executing such scheme and artifice.

98. Specifically, an object of the conspiracy was to gain unauthorized access into the computer networks of Westinghouse Electric Company (WEC), the U.S. Anti-Doping Agency (USADA), the World Anti-Doping Agency (WADA), and the Canadian Center for Ethics in Sport (CCES) as well as the personal and business email accounts of their respective employees, in order to steal user login credentials and passwords, email communications, personally identifiable information, sensitive medical information of international athletes, proprietary information, data, property and other information of value, by means of false and fraudulent pretenses, to further the interests of the Russian Federation.

99. In order to gain unauthorized access to victims' email accounts and computer networks, defendants IVAN SERGEYEVICH YERMAKOV, ARTEM ANDREYEVICH MALYSHEV, ALEKSEI SERGEYEVICH MORENETS and EVGENII MIKHAYLOVICH SEREBRIAKOV, together with their conspirators, crafted and transmitted, in interstate and foreign commerce, spearphishing emails that targeted the victims. The spearphishing emails were designed to appear legitimate in order to deceive recipient victims into opening the email and clicking on a malicious attachment or link that, when clicked, enabled the conspirators to steal the victims' login credentials to gain access to the victims' networks. The malicious links included "spoofed," or mimicked, domains that resembled legitimate websites associated with the victim entities. For example, the conspirators registered the domain "Westinqhousenuclear" on December 10, 2014, "wada.awa.org" on August 3, 2016, and "wada.arna.org," and "tas-cass.org"

on August 8, 2016, and thereafter utilized those spoofed domains in furtherance of the fraud scheme.

All in violation of Title 18, United States Code, Sections 1349 and 3559(g)(1).

COUNTS THREE THROUGH SEVEN
(Wire Fraud)

The grand jury further charges:

100. The allegations contained in Paragraphs 1 through 94 of this Indictment are repeated, re-alleged, and incorporated by reference as if fully set forth herein.

101. On or about the dates set forth below, in the Western District of Pennsylvania and elsewhere, the defendant, IVAN SERGEYEVICH YERMAKOV, having devised and intending to devise a scheme and artifice to defraud, and to obtain property by means of false and fraudulent pretenses, representations and promises, did transmit and cause to be transmitted by means of wire communication in interstate and foreign commerce, certain writings, signs, signals, and pictures for the purpose of executing such scheme and artifice; to wit, the defendant did knowingly transmit spearphishing emails, designed to appear legitimate, that contained malicious Bit.ly links, to the personal email accounts of the victims identified below, all employees of Westinghouse Electric Company (WEC), on or about the dates set forth below, with the intention of obtaining the victims' account login credentials, with each such transmission being a separate count of this indictment:

Count	Approx. Date	Victim	Bit.ly Link	Bit.ly Account
3	December 24, 2014	A	http://bit.ly/16Q0fWb	activqwe
4	December 24, 2014	B	http://bit.ly/1xb8Efq	activqwe
5	December 24, 2014	C	http://bit.ly/13vFZqx	activqwe
6	January 17, 2015	D	http://bit.ly/1CiXN3W	activqwe
7	January 17, 2015	E	http://bit.ly/1Cz3Fqk	activqwe

All in violation of Title 18, United States Code, Sections 1343 and 2.

COUNTS EIGHT AND NINE
(Aggravated Identity Theft)

The grand jury further charges:

102. The allegations contained in Paragraphs 1 through 94 of this Indictment are repeated, re-alleged, and incorporated by reference as if fully set forth herein.

103. Beginning in at least November 2014 and continuing until at least September 2016, in the Western District of Pennsylvania and elsewhere, the defendants, ALEKSEI SERGEYEVICH MORENETS, EVGENII MIKHAYLOVICH SEREBRIAKOV, IVAN SERGEYEVICH YERMAKOV, ARTEM ANDREYEVICH MALYSHEV and DMITRIY SERGEYEVICH BADIN, aided and abetted by others known and unknown to the grand jury, did knowingly transfer, possess and use without lawful authority, a means of identification of another person during and in relation to a felony violation enumerated in Title 18, United States Code, Section 1028A(c), namely, conspiracy to commit wire fraud, in violation of Title 18, United States Code, Section 1349, knowing that the means of identification belonged to another real person who worked on behalf of the targeted victim organizations: Westinghouse Electric Company and the U.S. Anti-Doping Agency (USADA).

Count	Approx. Date	Victim Org.	Means of Identification
8	From November 2014- January 2015	WEC	Username and passwords for multiple employee accounts
9	September 6, 2016	USADA	Login credentials for USADA official

In violation of Title 18, United States Code, Sections 1028A(a)(1), 1028A(b), 1028(c)(4) and 2.

COUNT TEN

(Conspiracy to Commit Money Laundering)

The grand jury further charges:

104. The allegations contained in Paragraphs 1 through 94 of this Indictment are repeated, re-alleged, and incorporated by reference as if fully set forth herein.

105. To facilitate the purchase of infrastructure used in their hacking activity—targeting anti-doping and other sports-related organizations and releasing the stolen documents—defendants ALEKSEI SERGEYEVICH MORENETS, EVGENII MIKHAYLOVICH SEREBRIAKOV, IVAN SERGEYEVICH YERMAKOV, ARTEM ANDREYEVICH MALYSHEV, DMITRIY SERGEYEVICH BADIN, OLEG MIKHAYLOVICH SOTNIKOV and ALEXEY VALEREVICH MININ, together with conspirators known and unknown, conspired to launder money through a web of transactions structured to capitalize on the perceived anonymity of cryptocurrencies such as bitcoin.

106. Although the conspirators caused transactions to be conducted in a variety of currencies, including U.S. dollars, they principally used bitcoin when purchasing servers, registering domains, and otherwise making payments in furtherance of hacking activity. Many of these payments were processed by companies located in the United States that provided payment processing services to hosting companies, domain registrars, and other vendors both international and domestic. The use of bitcoin allowed the conspirators to avoid direct relationships with traditional financial institutions, allowing them to evade greater scrutiny of their identities and sources of funds.

107. All bitcoin transactions are added to a public ledger called the Blockchain, but the Blockchain identifies the parties to each transaction only by alpha-numeric identifiers known as

bitcoin addresses. To further avoid creating a centralized paper trail of all of their purchases, the conspirators purchased infrastructure using hundreds of different email accounts, in some cases using a new account for each purchase. The conspirators used fictitious names and addresses in order to obscure their identities and their links to Russia and the Russian government. For example, the wada.arna.org, tas-cass.org domains and an associated virtual private server were registered and paid for using the fictitious name “Beula Town.”

108. The conspirators used several dedicated email accounts to track basic bitcoin transaction information and to facilitate bitcoin payments to vendors. One of these dedicated accounts received hundreds of bitcoin payment requests from approximately 100 different email accounts. For example, on or about August 8, 2016, the account received the instruction to “[p]lease send exactly 0.012684 bitcoin to” a certain thirty-four character bitcoin address. Shortly thereafter, a transaction matching those exact instructions was added to the Blockchain.

109. On occasion, the conspirators facilitated bitcoin payments using the same computers that they used to conduct their hacking activity, including to create and send test spearphishing emails.

110. The conspirators funded the purchase of computer infrastructure for their hacking activity in part by “mining” bitcoin. Individuals and entities can mine bitcoin by allowing their computing power to be used to verify and record payments on the bitcoin public ledger, a service for which they are rewarded with freshly-minted bitcoin. The pool of bitcoin generated from the GRU’s mining activity was used, for example, to pay a United States-based company to register the domain wada-arna.org through a payment processing company located in the United States.

111. The conspirators used the same funding structure—and in some cases, the very same pool of funds—to purchase key accounts, servers, and domains used in their anti-doping-related hacking activity. For example, the conspirators used the same pool of bitcoins to fund two operational personas which, in turn, registered the domains wada-arna.org (to target WADA), tas-cass.org (to target TAS/CAS) and the domains upmonserv.net and appexrv.com, used for command and control of X-agent malware installed on CCES network.

STATUTORY ALLEGATIONS

112. From at least in or around 2015 through 2016, within the Western District of Pennsylvania and elsewhere, defendants ALEKSEI SERGEYEVICH MORENETS, EVGENII MIKHAYLOVICH SEREBRIAKOV, IVAN SERGEYEVICH YERMAKOV, ARTEM ANDREYEVICH MALYSHEV, DMITRIY SERGEYEVICH BADIN, OLEG MIKHAYLOVICH SOTNIKOV and ALEXEY VALEREVICH MININ, together with others, known and unknown to the grand jury, did knowingly and intentionally conspire to transport, transmit, and transfer monetary instruments and funds to a place in the United States from and through a place outside the United States, with the intent to promote the carrying on of specified unlawful activity, namely, a violation of Title 18, United States Code, Section 1030, contrary to Title 18, United States Code, Section 1956(a)(2)(A).

All in violation of Title 18, United States Code, Section 1956(h).

FORFEITURE ALLEGATIONS


113. The allegations contained in Counts One through Ten of this Indictment are incorporated herein by reference as though fully set forth herein for the purpose of alleging criminal forfeitures pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i)(1)(A).

114. As a result of the commission of the violations charged in Count One, the defendants, ALEKSEI SERGEYEVICH MORENETS, EVGENII MIKHAYLOVICH SEREBRIAKOV, IVAN SERGEYEVICH YERMAKOV, ARTEM ANDREYEVICH MALYSHEV, DMITRIY SERGEYEVICH BADIN, OLEG MIKHAYLOVICH SOTNIKOV and ALEXEY VALEREVICH MININ, did use the following to commit or to promote the commission of said violations (hereinafter collectively referred to as the "Subject Domain Names"): fancybear.net and fancybear.org.

115. The United States hereby gives notice to the defendants, ALEKSEI SERGEYEVICH MORENETS, EVGENII MIKHAYLOVICH SEREBRIAKOV, IVAN SERGEYEVICH YERMAKOV, ARTEM ANDREYEVICH MALYSHEV, DMITRIY SERGEYEVICH BADIN, OLEG MIKHAYLOVICH SOTNIKOV and ALEXEY VALEREVICH MININ, charged in Count One that, upon their conviction of such offense, the government will seek forfeiture in accordance with: (a) Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i)(1)(B), which require any person convicted of such offense to forfeit any property constituting or derived from proceeds obtained directly or indirectly as a result of such offense; and (b) Title 18, United States Code, Section 1030(i)(1)(A), which requires any person convicted of such offense to forfeit any personal property that was used or intended to be used to

commit or to facilitate the commission of the offense, including but not limited to the following

SUBJECT DOMAIN NAMES: fancybear.net and fancybear.org.


SCOTT W. BRADY
United States Attorney
PA ID No. 88352

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA

v.

INTERNET RESEARCH AGENCY LLC
A/K/A MEDIASINTEZ LLC A/K/A
GLAVSET LLC A/K/A MIXINFO
LLC A/K/A AZIMUT LLC A/K/A
NOVINFO LLC,
CONCORD MANAGEMENT AND
CONSULTING LLC,
CONCORD CATERING,
YEVGENIY VIKTOROVICH
PRIGOZHIN,
MIKHAIL IVANOVICH BYSTROV,
MIKHAIL LEONIDOVICH BURCHIK
A/K/A MIKHAIL ABRAMOV,
ALEKSANDRA YURYEVNA
KRYLOVA,
ANNA VLADISLAVOVNA
BOGACHEVA,
SERGEY PAVLOVICH POLOZOV,
MARIA ANATOLYEVNA BOVDA
A/K/A MARIA ANATOLYEVNA
BELYAEVA,
ROBERT SERGEYEVICH BOVDA,
DZHEYKHUN NASIMI OGLY
ASLANOV A/K/A JAYHOON
ASLANOV A/K/A JAY ASLANOV,
VADIM VLADIMIROVICH
PODKOPAEV,
GLEB IGOREVICH VASILCHENKO,
IRINA VIKTOROVNA KAVERZINA,
and
VLADIMIR VENKOV.

CRIMINAL NO.

(18 U.S.C. §§ 2, 371, 1349, 1028A)

Defendants.

INDICTMENT

The Grand Jury for the District of Columbia charges:

Introduction

1. The United States of America, through its departments and agencies, regulates the activities of foreign individuals and entities in and affecting the United States in order to prevent, disclose, and counteract improper foreign influence on U.S. elections and on the U.S. political system. U.S. law bans foreign nationals from making certain expenditures or financial disbursements for the purpose of influencing federal elections. U.S. law also bars agents of any foreign entity from engaging in political activities within the United States without first registering with the Attorney General. And U.S. law requires certain foreign nationals seeking entry to the United States to obtain a visa by providing truthful and accurate information to the government. Various federal agencies, including the Federal Election Commission, the U.S. Department of Justice, and the U.S. Department of State, are charged with enforcing these laws.

2. Defendant INTERNET RESEARCH AGENCY LLC (“ORGANIZATION”) is a Russian organization engaged in operations to interfere with elections and political processes. Defendants MIKHAIL IVANOVICH BYSTROV, MIKHAIL LEONIDOVICH BURCHIK, ALEKSANDRA YURYEVNA KRYLOVA, ANNA VLADISLAVOVNA BOGACHEVA, SERGEY PAVLOVICH POLOZOV, MARIA ANATOLYEVNA BOVDA, ROBERT SERGEYEVICH BOVDA, DZHEYKHUN NASIMI OGLY ASLANOV, VADIM VLADIMIROVICH PODKOPAEV, GLEB IGOREVICH VASILCHENKO, IRINA VIKTOROVNA KAVERZINA, and VLADIMIR VENKOV worked in various capacities to carry out Defendant ORGANIZATION’s interference operations targeting the United States. From in or around 2014 to the present, Defendants knowingly and intentionally conspired with each other (and with persons known and unknown to

the Grand Jury) to defraud the United States by impairing, obstructing, and defeating the lawful functions of the government through fraud and deceit for the purpose of interfering with the U.S. political and electoral processes, including the presidential election of 2016.

3. Beginning as early as 2014, Defendant ORGANIZATION began operations to interfere with the U.S. political system, including the 2016 U.S. presidential election. Defendant ORGANIZATION received funding for its operations from Defendant YEVGENIY VIKTOROVICH PRIGOZHIN and companies he controlled, including Defendants CONCORD MANAGEMENT AND CONSULTING LLC and CONCORD CATERING (collectively “CONCORD”). Defendants CONCORD and PRIGOZHIN spent significant funds to further the ORGANIZATION’s operations and to pay the remaining Defendants, along with other uncharged ORGANIZATION employees, salaries and bonuses for their work at the ORGANIZATION.

4. Defendants, posing as U.S. persons and creating false U.S. personas, operated social media pages and groups designed to attract U.S. audiences. These groups and pages, which addressed divisive U.S. political and social issues, falsely claimed to be controlled by U.S. activists when, in fact, they were controlled by Defendants. Defendants also used the stolen identities of real U.S. persons to post on ORGANIZATION-controlled social media accounts. Over time, these social media accounts became Defendants’ means to reach significant numbers of Americans for purposes of interfering with the U.S. political system, including the presidential election of 2016.

5. Certain Defendants traveled to the United States under false pretenses for the purpose of collecting intelligence to inform Defendants’ operations. Defendants also procured and used computer infrastructure, based partly in the United States, to hide the Russian origin of their activities and to avoid detection by U.S. regulators and law enforcement.

6. Defendant ORGANIZATION had a strategic goal to sow discord in the U.S. political system, including the 2016 U.S. presidential election. Defendants posted derogatory information about a number of candidates, and by early to mid-2016, Defendants' operations included supporting the presidential campaign of then-candidate Donald J. Trump ("Trump Campaign") and disparaging Hillary Clinton. Defendants made various expenditures to carry out those activities, including buying political advertisements on social media in the names of U.S. persons and entities. Defendants also staged political rallies inside the United States, and while posing as U.S. grassroots entities and U.S. persons, and without revealing their Russian identities and ORGANIZATION affiliation, solicited and compensated real U.S. persons to promote or disparage candidates. Some Defendants, posing as U.S. persons and without revealing their Russian association, communicated with unwitting individuals associated with the Trump Campaign and with other political activists to seek to coordinate political activities.

7. In order to carry out their activities to interfere in U.S. political and electoral processes without detection of their Russian affiliation, Defendants conspired to obstruct the lawful functions of the United States government through fraud and deceit, including by making expenditures in connection with the 2016 U.S. presidential election without proper regulatory disclosure; failing to register as foreign agents carrying out political activities within the United States; and obtaining visas through false and fraudulent statements.

COUNT ONE

(Conspiracy to Defraud the United States)

8. Paragraphs 1 through 7 of this Indictment are re-alleged and incorporated by reference as if fully set forth herein.

9. From in or around 2014 to the present, in the District of Columbia and elsewhere,

Defendants, together with others known and unknown to the Grand Jury, knowingly and intentionally conspired to defraud the United States by impairing, obstructing, and defeating the lawful functions of the Federal Election Commission, the U.S. Department of Justice, and the U.S. Department of State in administering federal requirements for disclosure of foreign involvement in certain domestic activities.

Defendants

10. Defendant INTERNET RESEARCH AGENCY LLC (Агентство Интернет Исследований) is a Russian organization engaged in political and electoral interference operations. In or around July 2013, the ORGANIZATION registered with the Russian government as a Russian corporate entity. Beginning in or around June 2014, the ORGANIZATION obscured its conduct by operating through a number of Russian entities, including Internet Research LLC, MediaSintez LLC, GlavSet LLC, MixInfo LLC, Azimut LLC, and NovInfo LLC. Starting in or around 2014, the ORGANIZATION occupied an office at 55 Savushkina Street in St. Petersburg, Russia. That location became one of the ORGANIZATION's operational hubs from which Defendants and other co-conspirators carried out their activities to interfere in the U.S. political system, including the 2016 U.S. presidential election.

- a. The ORGANIZATION employed hundreds of individuals for its online operations, ranging from creators of fictitious personas to technical and administrative support. The ORGANIZATION's annual budget totaled the equivalent of millions of U.S. dollars.
- b. The ORGANIZATION was headed by a management group and organized into departments, including: a graphics department; a data analysis department; a search-engine optimization ("SEO") department; an information-technology ("IT")

department to maintain the digital infrastructure used in the ORGANIZATION's operations; and a finance department to budget and allocate funding.

- c. The ORGANIZATION sought, in part, to conduct what it called "information warfare against the United States of America" through fictitious U.S. personas on social media platforms and other Internet-based media.
- d. By in or around April 2014, the ORGANIZATION formed a department that went by various names but was at times referred to as the "translator project." This project focused on the U.S. population and conducted operations on social media platforms such as YouTube, Facebook, Instagram, and Twitter. By approximately July 2016, more than eighty ORGANIZATION employees were assigned to the translator project.
- e. By in or around May 2014, the ORGANIZATION's strategy included interfering with the 2016 U.S. presidential election, with the stated goal of "spread[ing] distrust towards the candidates and the political system in general."

11. Defendants CONCORD MANAGEMENT AND CONSULTING LLC (Конкорд Менеджмент и Консалтинг) and CONCORD CATERING are related Russian entities with various Russian government contracts. CONCORD was the ORGANIZATION's primary source of funding for its interference operations. CONCORD controlled funding, recommended personnel, and oversaw ORGANIZATION activities through reporting and interaction with ORGANIZATION management.

- a. CONCORD funded the ORGANIZATION as part of a larger CONCORD-funded interference operation that it referred to as "Project Lakhta." Project Lakhta had multiple components, some involving domestic audiences within the Russian

Federation and others targeting foreign audiences in various countries, including the United States.

- b. By in or around September 2016, the ORGANIZATION's monthly budget for Project Lakhta submitted to CONCORD exceeded 73 million Russian rubles (over 1,250,000 U.S. dollars), including approximately one million rubles in bonus payments.
- c. To conceal its involvement, CONCORD labeled the monies paid to the ORGANIZATION for Project Lakhta as payments related to software support and development. To further conceal the source of funds, CONCORD distributed monies to the ORGANIZATION through approximately fourteen bank accounts held in the names of CONCORD affiliates, including Glavnaya Liniya LLC, Mercuriy LLC, Obshchepit LLC, Potentsial LLC, RSP LLC, ASP LLC, MTTs LLC, Kompleksservis LLC, SPb Kulinariya LLC, Almira LLC, Pishchevik LLC, Galant LLC, Rayteks LLC, and Standart LLC.

12. Defendant YEVGENIY VIKTOROVICH PRIGOZHIN (Пригожин Евгений Викторович) is a Russian national who controlled CONCORD.

- a. PRIGOZHIN approved and supported the ORGANIZATION's operations, and Defendants and their co-conspirators were aware of PRIGOZHIN's role.
- b. For example, on or about May 29, 2016, Defendants and their co-conspirators, through an ORGANIZATION-controlled social media account, arranged for a real U.S. person to stand in front of the White House in the District of Columbia under false pretenses to hold a sign that read "Happy 55th Birthday Dear Boss." Defendants and their co-conspirators informed the real U.S. person that the sign

was for someone who “is a leader here and our boss . . . our funder.” PRIGOZHIN’s Russian passport identifies his date of birth as June 1, 1961.

13. Defendant MIKHAIL IVANOVICH BYSTROV (Быстров Михаил Иванович) joined the ORGANIZATION by at least in or around February 2014.

a. By approximately April 2014, BYSTROV was the general director, the ORGANIZATION’s highest-ranking position. BYSTROV subsequently served as the head of various other entities used by the ORGANIZATION to mask its activities, including, for example, Glavset LLC, where he was listed as that entity’s general director.

b. In or around 2015 and 2016, BYSTROV frequently communicated with PRIGOZHIN about Project Lakhta’s overall operations, including through regularly scheduled in-person meetings.

14. Defendant MIKHAIL LEONIDOVICH BURCHIK (Бурчик Михаил Леонидович) A/K/A MIKHAIL ABRAMOV joined the ORGANIZATION by at least in or around October 2013. By approximately March 2014, BURCHIK was the executive director, the ORGANIZATION’s second-highest ranking position. Throughout the ORGANIZATION’s operations to interfere in the U.S political system, including the 2016 U.S. presidential election, BURCHIK was a manager involved in operational planning, infrastructure, and personnel. In or around 2016, BURCHIK also had in-person meetings with PRIGOZHIN.

15. Defendant ALEKSANDRA YURYEVNA KRYLOVA (Крылова Александра Юрьевна) worked for the ORGANIZATION from at least in or around September 2013 to at least in or around November 2014. By approximately April 2014, KRYLOVA served as director and was the ORGANIZATION’s third-highest ranking employee. In 2014, KRYLOVA traveled to the United

States under false pretenses for the purpose of collecting intelligence to inform the ORGANIZATION's operations.

16. Defendant SERGEY PAVLOVICH POLOZOV (Полозов Сергей Павлович) worked for the ORGANIZATION from at least in or around April 2014 to at least in or around October 2016. POLOZOV served as the manager of the IT department and oversaw the procurement of U.S. servers and other computer infrastructure that masked the ORGANIZATION's Russian location when conducting operations within the United States.

17. Defendant ANNA VLADISLAVOVNA BOGACHEVA (Богачева Анна Владиславовна) worked for the ORGANIZATION from at least in or around April 2014 to at least in or around July 2014. BOGACHEVA served on the translator project and oversaw the project's data analysis group. BOGACHEVA also traveled to the United States under false pretenses for the purpose of collecting intelligence to inform the ORGANIZATION's operations.

18. Defendant MARIA ANATOLYEVNA BOVDA (Бовда Мария Анатольевна) A/K/A MARIA ANATOLYEVNA BELYAEVA ("M. BOVDA") worked for the ORGANIZATION from at least in or around November 2013 to at least in or around October 2014. M. BOVDA served as the head of the translator project, among other positions.

19. Defendant ROBERT SERGEYEVICH BOVDA (Бовда Роберт Сергеевич) ("R. BOVDA") worked for the ORGANIZATION from at least in or around November 2013 to at least in or around October 2014. R. BOVDA served as the deputy head of the translator project, among other positions. R. BOVDA attempted to travel to the United States under false pretenses for the purpose of collecting intelligence to inform the ORGANIZATION's operations but could not obtain the necessary visa.

20. Defendant DZHEYKHUN NASIMI OGLY ASLANOV (Асланов Джейхун Насими Оглы) A/K/A JAYHOON ASLANOV A/K/A JAY ASLANOV joined the ORGANIZATION by at least in or around September 2014. ASLANOV served as head of the translator project and oversaw many of the operations targeting the 2016 U.S. presidential election. ASLANOV was also listed as the general director of Azimut LLC, an entity used to move funds from CONCORD to the ORGANIZATION.

21. Defendant VADIM VLADIMIROVICH PODKOPEV (Подкопеев Вадим Владимирович) joined the ORGANIZATION by at least in or around June 2014. PODKOPEV served as an analyst on the translator project and was responsible for conducting U.S.-focused research and drafting social media content for the ORGANIZATION.

22. Defendant GLEB IGOREVICH VASILCHENKO (Васильченко Глеб Игоревич) worked for the ORGANIZATION from at least in or around August 2014 to at least in or around September 2016. VASILCHENKO was responsible for posting, monitoring, and updating the social media content of many ORGANIZATION-controlled accounts while posing as U.S. persons or U.S. grassroots organizations. VASILCHENKO later served as the head of two sub-groups focused on operations to interfere in the U.S. political system, including the 2016 U.S. presidential election.

23. Defendant IRINA VIKTOROVNA KAVERZINA (Каверзина Ирина Викторовна) joined the ORGANIZATION by at least in or around October 2014. KAVERZINA served on the translator project and operated multiple U.S. personas that she used to post, monitor, and update social media content for the ORGANIZATION.

24. Defendant VLADIMIR VENKOV (Венков Владимир) joined the ORGANIZATION by at least in or around March 2015. VENKOV served on the translator project and operated multiple

U.S. personas, which he used to post, monitor, and update social media content for the ORGANIZATION.

Federal Regulatory Agencies

25. The Federal Election Commission is a federal agency that administers the Federal Election Campaign Act (“FECA”). Among other things, FECA prohibits foreign nationals from making any contributions, expenditures, independent expenditures, or disbursements for electioneering communications. FECA also requires that individuals or entities who make certain independent expenditures in federal elections report those expenditures to the Federal Election Commission. The reporting requirements permit the Federal Election Commission to fulfill its statutory duties of providing the American public with accurate data about the financial activities of individuals and entities supporting federal candidates, and enforcing FECA’s limits and prohibitions, including the ban on foreign expenditures.

26. The U.S. Department of Justice administers the Foreign Agent Registration Act (“FARA”). FARA establishes a registration, reporting, and disclosure regime for agents of foreign principals (which includes foreign non-government individuals and entities) so that the U.S. government and the people of the United States are informed of the source of information and the identity of persons attempting to influence U.S. public opinion, policy, and law. FARA requires, among other things, that persons subject to its requirements submit periodic registration statements containing truthful information about their activities and the income earned from them. Disclosure of the required information allows the federal government and the American people to evaluate the statements and activities of such persons in light of their function as foreign agents.

27. The U.S. Department of State is the federal agency responsible for the issuance of non-immigrant visas to foreign individuals who need a visa to enter the United States. Foreign

individuals who are required to obtain a visa must, among other things, provide truthful information in response to questions on the visa application form, including information about their employment and the purpose of their visit to the United States.

Object of the Conspiracy

28. The conspiracy had as its object impairing, obstructing, and defeating the lawful governmental functions of the United States by dishonest means in order to enable the Defendants to interfere with U.S. political and electoral processes, including the 2016 U.S. presidential election.

Manner and Means of the Conspiracy

Intelligence-Gathering to Inform U.S. Operations

29. Starting at least in or around 2014, Defendants and their co-conspirators began to track and study groups on U.S. social media sites dedicated to U.S. politics and social issues. In order to gauge the performance of various groups on social media sites, the ORGANIZATION tracked certain metrics like the group's size, the frequency of content placed by the group, and the level of audience engagement with that content, such as the average number of comments or responses to a post.

30. Defendants and their co-conspirators also traveled, and attempted to travel, to the United States under false pretenses in order to collect intelligence for their interference operations.

- a. KRYLOVA and BOGACHEVA, together with other Defendants and co-conspirators, planned travel itineraries, purchased equipment (such as cameras, SIM cards, and drop phones), and discussed security measures (including "evacuation scenarios") for Defendants who traveled to the United States.
- b. To enter the United States, KRYLOVA, BOGACHEVA, R. BOVDA, and another co-conspirator applied to the U.S. Department of State for visas to travel. During

their application process, KRYLOVA, BOGACHEVA, R. BOVDA, and their co-conspirator falsely claimed they were traveling for personal reasons and did not fully disclose their place of employment to hide the fact that they worked for the ORGANIZATION.

- c. Only KRYLOVA and BOGACHEVA received visas, and from approximately June 4, 2014 through June 26, 2014, KRYLOVA and BOGACHEVA traveled in and around the United States, including stops in Nevada, California, New Mexico, Colorado, Illinois, Michigan, Louisiana, Texas, and New York to gather intelligence. After the trip, KRYLOVA and BURCHIK exchanged an intelligence report regarding the trip.
- d. Another co-conspirator who worked for the ORGANIZATION traveled to Atlanta, Georgia from approximately November 26, 2014 through November 30, 2014. Following the trip, the co-conspirator provided POLOZOV a summary of his trip's itinerary and expenses.

31. In order to collect additional intelligence, Defendants and their co-conspirators posed as U.S. persons and contacted U.S. political and social activists. For example, starting in or around June 2016, Defendants and their co-conspirators, posing online as U.S. persons, communicated with a real U.S. person affiliated with a Texas-based grassroots organization. During the exchange, Defendants and their co-conspirators learned from the real U.S. person that they should focus their activities on "purple states like Colorado, Virginia & Florida." After that exchange, Defendants and their co-conspirators commonly referred to targeting "purple states" in directing their efforts.

Use of U.S. Social Media Platforms

32. Defendants and their co-conspirators, through fraud and deceit, created hundreds of social media accounts and used them to develop certain fictitious U.S. personas into “leader[s] of public opinion” in the United States.

33. ORGANIZATION employees, referred to as “specialists,” were tasked to create social media accounts that appeared to be operated by U.S. persons. The specialists were divided into day-shift and night-shift hours and instructed to make posts in accordance with the appropriate U.S. time zone. The ORGANIZATION also circulated lists of U.S. holidays so that specialists could develop and post appropriate account activity. Specialists were instructed to write about topics germane to the United States such as U.S. foreign policy and U.S. economic issues. Specialists were directed to create “political intensity through supporting radical groups, users dissatisfied with [the] social and economic situation and oppositional social movements.”

34. Defendants and their co-conspirators also created thematic group pages on social media sites, particularly on the social media platforms Facebook and Instagram. ORGANIZATION-controlled pages addressed a range of issues, including: immigration (with group names including “Secured Borders”); the Black Lives Matter movement (with group names including “Blacktivist”); religion (with group names including “United Muslims of America” and “Army of Jesus”); and certain geographic regions within the United States (with group names including “South United” and “Heart of Texas”). By 2016, the size of many ORGANIZATION-controlled groups had grown to hundreds of thousands of online followers.

35. Starting at least in or around 2015, Defendants and their co-conspirators began to purchase advertisements on online social media sites to promote ORGANIZATION-controlled social media groups, spending thousands of U.S. dollars every month. These expenditures were included in the budgets the ORGANIZATION submitted to CONCORD.

36. Defendants and their co-conspirators also created and controlled numerous Twitter accounts designed to appear as if U.S. persons or groups controlled them. For example, the ORGANIZATION created and controlled the Twitter account “Tennessee GOP,” which used the handle @TEN_GOP. The @TEN_GOP account falsely claimed to be controlled by a U.S. state political party. Over time, the @TEN_GOP account attracted more than 100,000 online followers.

37. To measure the impact of their online social media operations, Defendants and their co-conspirators tracked the performance of content they posted over social media. They tracked the size of the online U.S. audiences reached through posts, different types of engagement with the posts (such as likes, comments, and reposts), changes in audience size, and other metrics. Defendants and their co-conspirators received and maintained metrics reports on certain group pages and individualized posts.

38. Defendants and their co-conspirators also regularly evaluated the content posted by specialists (sometimes referred to as “content analysis”) to ensure they appeared authentic—as if operated by U.S. persons. Specialists received feedback and directions to improve the quality of their posts. Defendants and their co-conspirators issued or received guidance on: ratios of text, graphics, and video to use in posts; the number of accounts to operate; and the role of each account (for example, differentiating a main account from which to post information and auxiliary accounts to promote a main account through links and reposts).

Use of U.S. Computer Infrastructure

39. To hide their Russian identities and ORGANIZATION affiliation, Defendants and their co-conspirators—particularly POLOZOV and the ORGANIZATION’s IT department—purchased space on computer servers located inside the United States in order to set up virtual private networks (“VPNs”). Defendants and their co-conspirators connected from Russia to the U.S.-

based infrastructure by way of these VPNs and conducted activity inside the United States—including accessing online social media accounts, opening new accounts, and communicating with real U.S. persons—while masking the Russian origin and control of the activity.

40. Defendants and their co-conspirators also registered and controlled hundreds of web-based email accounts hosted by U.S. email providers under false names so as to appear to be U.S. persons and groups. From these accounts, Defendants and their co-conspirators registered or linked to online social media accounts in order to monitor them; posed as U.S. persons when requesting assistance from real U.S. persons; contacted media outlets in order to promote activities inside the United States; and conducted other operations, such as those set forth below.

Use of Stolen U.S. Identities

41. In or around 2016, Defendants and their co-conspirators also used, possessed, and transferred, without lawful authority, the social security numbers and dates of birth of real U.S. persons without those persons' knowledge or consent. Using these means of identification, Defendants and their co-conspirators opened accounts at PayPal, a digital payment service provider; created false means of identification, including fake driver's licenses; and posted on ORGANIZATION-controlled social media accounts using the identities of these U.S. victims. Defendants and their co-conspirators also obtained, and attempted to obtain, false identification documents to use as proof of identity in connection with maintaining accounts and purchasing advertisements on social media sites.

Actions Targeting the 2016 U.S. Presidential Election

42. By approximately May 2014, Defendants and their co-conspirators discussed efforts to interfere in the 2016 U.S. presidential election. Defendants and their co-conspirators began to monitor U.S. social media accounts and other sources of information about the 2016 U.S. presidential election.

43. By 2016, Defendants and their co-conspirators used their fictitious online personas to interfere with the 2016 U.S. presidential election. They engaged in operations primarily intended to communicate derogatory information about Hillary Clinton, to denigrate other candidates such as Ted Cruz and Marco Rubio, and to support Bernie Sanders and then-candidate Donald Trump.

- a. On or about February 10, 2016, Defendants and their co-conspirators internally circulated an outline of themes for future content to be posted to ORGANIZATION-controlled social media accounts. Specialists were instructed to post content that focused on “politics in the USA” and to “use any opportunity to criticize Hillary and the rest (except Sanders and Trump—we support them).”
- b. On or about September 14, 2016, in an internal review of an ORGANIZATION-created and controlled Facebook group called “Secured Borders,” the account specialist was criticized for having a “low number of posts dedicated to criticizing Hillary Clinton” and was told “it is imperative to intensify criticizing Hillary Clinton” in future posts.

44. Certain ORGANIZATION-produced materials about the 2016 U.S. presidential election used election-related hashtags, including: “#Trump2016,” “#TrumpTrain,” “#MAGA,” “#IWontProtectHillary,” and “#Hillary4Prison.” Defendants and their co-conspirators also established additional online social media accounts dedicated to the 2016 U.S. presidential election, including the Twitter account “March for Trump” and Facebook accounts “Clinton FRAUDation” and “Trumpsters United.”

45. Defendants and their co-conspirators also used false U.S. personas to communicate with unwitting members, volunteers, and supporters of the Trump Campaign involved in local community outreach, as well as grassroots groups that supported then-candidate Trump. These

individuals and entities at times distributed the ORGANIZATION's materials through their own accounts via retweets, reposts, and similar means. Defendants and their co-conspirators then monitored the propagation of content through such participants.

46. In or around the latter half of 2016, Defendants and their co-conspirators, through their ORGANIZATION-controlled personas, began to encourage U.S. minority groups not to vote in the 2016 U.S. presidential election or to vote for a third-party U.S. presidential candidate.

- a. On or about October 16, 2016, Defendants and their co-conspirators used the ORGANIZATION-controlled Instagram account "Woke Blacks" to post the following message: "[A] particular hype and hatred for Trump is misleading the people and forcing Blacks to vote Killary. We cannot resort to the lesser of two devils. Then we'd surely be better off without voting AT ALL."
- b. On or about November 3, 2016, Defendants and their co-conspirators purchased an advertisement to promote a post on the ORGANIZATION-controlled Instagram account "Blacktivist" that read in part: "Choose peace and vote for Jill Stein. Trust me, it's not a wasted vote."
- c. By in or around early November 2016, Defendants and their co-conspirators used the ORGANIZATION-controlled "United Muslims of America" social media accounts to post anti-vote messages such as: "American Muslims [are] boycotting elections today, most of the American Muslim voters refuse to vote for Hillary Clinton because she wants to continue the war on Muslims in the middle east and voted yes for invading Iraq."

47. Starting in or around the summer of 2016, Defendants and their co-conspirators also began to promote allegations of voter fraud by the Democratic Party through their fictitious U.S. personas

and groups on social media. Defendants and their co-conspirators purchased advertisements on Facebook to further promote the allegations.

- a. On or about August 4, 2016, Defendants and their co-conspirators began purchasing advertisements that promoted a post on the ORGANIZATION-controlled Facebook account “Stop A.I.” The post alleged that “Hillary Clinton has already committed voter fraud during the Democrat Iowa Caucus.”
- b. On or about August 11, 2016, Defendants and their co-conspirators posted that allegations of voter fraud were being investigated in North Carolina on the ORGANIZATION-controlled Twitter account @TEN_GOP.
- c. On or about November 2, 2016, Defendants and their co-conspirators used the same account to post allegations of “#VoterFraud by counting tens of thousands of ineligible mail in Hillary votes being reported in Broward County, Florida.”

Political Advertisements

48. From at least April 2016 through November 2016, Defendants and their co-conspirators, while concealing their Russian identities and ORGANIZATION affiliation through false personas, began to produce, purchase, and post advertisements on U.S. social media and other online sites expressly advocating for the election of then-candidate Trump or expressly opposing Clinton. Defendants and their co-conspirators did not report their expenditures to the Federal Election Commission, or register as foreign agents with the U.S. Department of Justice.

49. To pay for the political advertisements, Defendants and their co-conspirators established various Russian bank accounts and credit cards, often registered in the names of fictitious U.S. personas created and used by the ORGANIZATION on social media. Defendants and their co-conspirators also paid for other political advertisements using PayPal accounts.

50. The political advertisements included the following:

Approximate Date	Excerpt of Advertisement
April 6, 2016	"You know, a great number of black people support us saying that #HillaryClintonIsNotMyPresident"
April 7, 2016	"I say no to Hillary Clinton / I say no to manipulation"
April 19, 2016	"JOIN our #HillaryClintonForPrison2016"
May 10, 2016	"Donald wants to defeat terrorism . . . Hillary wants to sponsor it"
May 19, 2016	"Vote Republican, vote Trump, and support the Second Amendment!"
May 24, 2016	"Hillary Clinton Doesn't Deserve the Black Vote"
June 7, 2016	"Trump is our only hope for a better future!"
June 30, 2016	"#NeverHillary #HillaryForPrison #Hillary4Prison #HillaryForPrison2016 #Trump2016 #Trump #Trump4President"
July 20, 2016	"Ohio Wants Hillary 4 Prison"
August 4, 2016	"Hillary Clinton has already committed voter fraud during the Democrat Iowa Caucus."
August 10, 2016	"We cannot trust Hillary to take care of our veterans!"
October 14, 2016	"Among all the candidates Donald Trump is the one and only who can defend the police from terrorists."
October 19, 2016	"Hillary is a Satan, and her crimes and lies had proved just how evil she is."

Staging U.S. Political Rallies in the United States

51. Starting in approximately June 2016, Defendants and their co-conspirators organized and coordinated political rallies in the United States. To conceal the fact that they were based in Russia, Defendants and their co-conspirators promoted these rallies while pretending to be U.S. grassroots activists who were located in the United States but unable to meet or participate in person.

Defendants and their co-conspirators did not register as foreign agents with the U.S. Department of Justice.

52. In order to build attendance for the rallies, Defendants and their co-conspirators promoted the events through public posts on their false U.S. persona social media accounts. In addition, Defendants and their co-conspirators contacted administrators of large social media groups focused on U.S. politics and requested that they advertise the rallies.

53. In or around late June 2016, Defendants and their co-conspirators used the Facebook group “United Muslims of America” to promote a rally called “Support Hillary. Save American Muslims” held on July 9, 2016 in the District of Columbia. Defendants and their co-conspirators recruited a real U.S. person to hold a sign depicting Clinton and a quote attributed to her stating “I think Sharia Law will be a powerful new direction of freedom.” Within three weeks, on or about July 26, 2016, Defendants and their co-conspirators posted on the same Facebook page that Muslim voters were “between Hillary Clinton and a hard place.”

54. In or around June and July 2016, Defendants and their co-conspirators used the Facebook group “Being Patriotic,” the Twitter account @March_for_Trump, and other ORGANIZATION accounts to organize two political rallies in New York. The first rally was called “March for Trump” and held on June 25, 2016. The second rally was called “Down with Hillary” and held on July 23, 2016.

- a. In or around June through July 2016, Defendants and their co-conspirators purchased advertisements on Facebook to promote the “March for Trump” and “Down with Hillary” rallies.
- b. Defendants and their co-conspirators used false U.S. personas to send individualized messages to real U.S. persons to request that they participate in and

help organize the rally. To assist their efforts, Defendants and their co-conspirators, through false U.S. personas, offered money to certain U.S. persons to cover rally expenses.

- c. On or about June 5, 2016, Defendants and their co-conspirators, while posing as a U.S. grassroots activist, used the account @March_for_Trump to contact a volunteer for the Trump Campaign in New York. The volunteer agreed to provide signs for the “March for Trump” rally.

55. In or around late July 2016, Defendants and their co-conspirators used the Facebook group “Being Patriotic,” the Twitter account @March_for_Trump, and other false U.S. personas to organize a series of coordinated rallies in Florida. The rallies were collectively referred to as “Florida Goes Trump” and held on August 20, 2016.

- a. In or around August 2016, Defendants and their co-conspirators used false U.S. personas to communicate with Trump Campaign staff involved in local community outreach about the “Florida Goes Trump” rallies.
- b. Defendants and their co-conspirators purchased advertisements on Facebook and Instagram to promote the “Florida Goes Trump” rallies.
- c. Defendants and their co-conspirators also used false U.S. personas to contact multiple grassroots groups supporting then-candidate Trump in an unofficial capacity. Many of these groups agreed to participate in the “Florida Goes Trump” rallies and serve as local coordinators.
- d. Defendants and their co-conspirators also used false U.S. personas to ask real U.S. persons to participate in the “Florida Goes Trump” rallies. Defendants and their co-conspirators asked certain of these individuals to perform tasks at the rallies.

For example, Defendants and their co-conspirators asked one U.S. person to build a cage on a flatbed truck and another U.S. person to wear a costume portraying Clinton in a prison uniform. Defendants and their co-conspirators paid these individuals to complete the requests.

56. After the rallies in Florida, Defendants and their co-conspirators used false U.S. personas to organize and coordinate U.S. political rallies supporting then-candidate Trump in New York and Pennsylvania. Defendants and their co-conspirators used the same techniques to build and promote these rallies as they had in Florida, including: buying Facebook advertisements; paying U.S. persons to participate in, or perform certain tasks at, the rallies; and communicating with real U.S. persons and grassroots organizations supporting then-candidate Trump.

57. After the election of Donald Trump in or around November 2016, Defendants and their co-conspirators used false U.S. personas to organize and coordinate U.S. political rallies in support of then president-elect Trump, while simultaneously using other false U.S. personas to organize and coordinate U.S. political rallies protesting the results of the 2016 U.S. presidential election. For example, in or around November 2016, Defendants and their co-conspirators organized a rally in New York through one ORGANIZATION-controlled group designed to “show your support for President-Elect Donald Trump” held on or about November 12, 2016. At the same time, Defendants and their co-conspirators, through another ORGANIZATION-controlled group, organized a rally in New York called “Trump is NOT my President” held on or about November 12, 2016. Similarly, Defendants and their co-conspirators organized a rally entitled “Charlotte Against Trump” in Charlotte, North Carolina, held on or about November 19, 2016.

Destruction of Evidence

58. In order to avoid detection and impede investigation by U.S. authorities of Defendants' operations, Defendants and their co-conspirators deleted and destroyed data, including emails, social media accounts, and other evidence of their activities.

- a. Beginning in or around June 2014, and continuing into June 2015, public reporting began to identify operations conducted by the ORGANIZATION in the United States. In response, Defendants and their co-conspirators deleted email accounts used to conduct their operations.
- b. Beginning in or around September 2017, U.S. social media companies, starting with Facebook, publicly reported that they had identified Russian expenditures on their platforms to fund political and social advertisements. Facebook's initial disclosure of the Russian purchases occurred on or about September 6, 2017, and included a statement that Facebook had "shared [its] findings with US authorities investigating these issues."
- c. Media reporting on or about the same day as Facebook's disclosure referred to Facebook working with investigators for the Special Counsel's Office of the U.S. Department of Justice, which had been charged with investigating the Russian government's efforts to interfere in the 2016 presidential election.
- d. Defendants and their co-conspirators thereafter destroyed evidence for the purpose of impeding the investigation. On or about September 13, 2017, KAVERZINA wrote in an email to a family member: "We had a slight crisis here at work: the FBI busted our activity (not a joke). So, I got preoccupied with covering tracks together with the colleagues." KAVERZINA further wrote, "I created all these pictures and posts, and the Americans believed that it was written by their people."

Overt Acts

59. In furtherance of the Conspiracy and to effect its illegal object, Defendants and their co-conspirators committed the following overt acts in connection with the staging of U.S. political rallies, as well as those as set forth in paragraphs 1 through 7, 9 through 27, and 29 through 58, which are re-alleged and incorporated by reference as though fully set forth herein.

60. On or about June 1, 2016, Defendants and their co-conspirators created and purchased Facebook advertisements for their “March for Trump” rally.

61. On or about June 4, 2016, Defendants and their co-conspirators used allforusa@yahoo.com, the email address of a false U.S. persona, to send out press releases for the “March for Trump” rally to New York media outlets.

62. On or about June 23, 2016, Defendants and their co-conspirators used the Facebook account registered under a false U.S. persona “Matt Skiber” to contact a real U.S. person to serve as a recruiter for the “March for Trump” rally, offering to “give you money to print posters and get a megaphone.”

63. On or about June 24, 2016, Defendants and their co-conspirators purchased advertisements on Facebook to promote the “Support Hillary. Save American Muslims” rally.

64. On or about July 5, 2016, Defendants and their co-conspirators ordered posters for the “Support Hillary. Save American Muslims” rally, including the poster with the quote attributed to Clinton that read “I think Sharia Law will be a powerful new direction of freedom.”

65. On or about July 8, 2016, Defendants and their co-conspirators communicated with a real U.S. person about the posters they had ordered for the “Support Hillary. Save American Muslims” rally.

66. On or about July 12, 2016, Defendants and their co-conspirators created and purchased Facebook advertisements for the “Down With Hillary” rally in New York.

67. On or about July 23, 2016, Defendants and their co-conspirators used the email address of a false U.S. persona, joshmilton024@gmail.com, to send out press releases to over thirty media outlets promoting the “Down With Hillary” rally at Trump Tower in New York City.

68. On or about July 28, 2016, Defendants and their co-conspirators posted a series of tweets through the false U.S. persona account @March_for_Trump stating that “[w]e’re currently planning a series of rallies across the state of Florida” and seeking volunteers to assist.

69. On or about August 2, 2016, Defendants and their co-conspirators used the false U.S. persona “Matt Skiber” Facebook account to send a private message to a real Facebook account, “Florida for Trump,” set up to assist then-candidate Trump in the state of Florida. In the first message, Defendants and their co-conspirators wrote:

Hi there! I’m a member of Being Patriotic online community. Listen, we’ve got an idea. Florida is still a purple state and we need to paint it red. If we lose Florida, we lose America. We can’t let it happen, right? What about organizing a YUGE pro-Trump flash mob in every Florida town? We are currently reaching out to local activists and we’ve got the folks who are okay to be in charge of organizing their events almost everywhere in FL. However, we still need your support. What do you think about that? Are you in?

70. On or about August 2, 2016, and August 3, 2016, Defendants and their co-conspirators, through the use of a stolen identity of a real U.S. person, T.W., sent emails to certain grassroots groups located in Florida that stated in part:

My name is [T.W.] and I represent a conservative patriot community named as “Being Patriotic.” . . . So we’re gonna organize a flash mob across Florida to support Mr. Trump. We clearly understand that the elections winner will be predestined by purple states. And we must win Florida. . . . We got a lot of volunteers in ~25 locations and it’s just the beginning. We’re currently choosing venues for each

location and recruiting more activists. This is why we ask you to spread this info and participate in the flash mob.

71. On or about August 4, 2016, Defendants and their co-conspirators created and purchased Facebook advertisements for the “Florida Goes Trump” rally. The advertisements reached over 59,000 Facebook users in Florida, and over 8,300 Facebook users responded to the advertisements by clicking on it, which routed users to the ORGANIZATION’s “Being Patriotic” page.

72. Beginning on or about August 5, 2016, Defendants and their co-conspirators used the false U.S. persona @March_for_Trump Twitter account to recruit and later pay a real U.S. person to wear a costume portraying Clinton in a prison uniform at a rally in West Palm Beach.

73. Beginning on or about August 11, 2016, Defendants and their co-conspirators used the false U.S. persona “Matt Skiber” Facebook account to recruit a real U.S. person to acquire signs and a costume depicting Clinton in a prison uniform.

74. On or about August 15, 2016, Defendants and their co-conspirators received an email at one of their false U.S. persona accounts from a real U.S. person, a Florida-based political activist identified as the “Chair for the Trump Campaign” in a particular Florida county. The activist identified two additional sites in Florida for possible rallies. Defendants and their co-conspirators subsequently used their false U.S. persona accounts to communicate with the activist about logistics and an additional rally in Florida.

75. On or about August 16, 2016, Defendants and their co-conspirators used a false U.S. persona Instagram account connected to the ORGANIZATION-created group “Tea Party News” to purchase advertisements for the “Florida Goes Trump” rally.

76. On or about August 18, 2016, the real “Florida for Trump” Facebook account responded to the false U.S. persona “Matt Skiber” account with instructions to contact a member of the Trump Campaign (“Campaign Official 1”) involved in the campaign’s Florida operations and provided

Campaign Official 1's email address at the campaign domain donaldtrump.com. On approximately the same day, Defendants and their co-conspirators used the email address of a false U.S. persona, joshmilton024@gmail.com, to send an email to Campaign Official 1 at that donaldtrump.com email account, which read in part:

Hello [Campaign Official 1], [w]e are organizing a state-wide event in Florida on August, 20 to support Mr. Trump. Let us introduce ourselves first. "Being Patriotic" is a grassroots conservative online movement trying to unite people offline. . . . [W]e gained a huge lot of followers and decided to somehow help Mr. Trump get elected. You know, simple yelling on the Internet is not enough. There should be real action. We organized rallies in New York before. Now we're focusing on purple states such as Florida.

The email also identified thirteen "confirmed locations" in Florida for the rallies and requested the campaign provide "assistance in each location."

77. On or about August 18, 2016, Defendants and their co-conspirators sent money via interstate wire to another real U.S. person recruited by the ORGANIZATION, using one of their false U.S. personas, to build a cage large enough to hold an actress depicting Clinton in a prison uniform.

78. On or about August 19, 2016, a supporter of the Trump Campaign sent a message to the ORGANIZATION-controlled "March for Trump" Twitter account about a member of the Trump Campaign ("Campaign Official 2") who was involved in the campaign's Florida operations and provided Campaign Official 2's email address at the domain donaldtrump.com. On or about the same day, Defendants and their co-conspirators used the false U.S. persona joshmilton024@gmail.com account to send an email to Campaign Official 2 at that donaldtrump.com email account.

79. On or about August 19, 2016, the real "Florida for Trump" Facebook account sent another message to the false U.S. persona "Matt Skiber" account to contact a member of the Trump

Campaign (“Campaign Official 3”) involved in the campaign’s Florida operations. On or about August 20, 2016, Defendants and their co-conspirators used the “Matt Skiber” Facebook account to contact Campaign Official 3.

80. On or about August 19, 2016, Defendants and their co-conspirators used the false U.S. persona “Matt Skiber” account to write to the real U.S. person affiliated with a Texas-based grassroots organization who previously had advised the false persona to focus on “purple states like Colorado, Virginia & Florida.” Defendants and their co-conspirators told that U.S. person, “We were thinking about your recommendation to focus on purple states and this is what we’re organizing in FL.” Defendants and their co-conspirators then sent a link to the Facebook event page for the Florida rallies and asked that person to send the information to Tea Party members in Florida. The real U.S. person stated that he/she would share among his/her own social media contacts, who would pass on the information.

81. On or about August 24, 2016, Defendants and their co-conspirators updated an internal ORGANIZATION list of over 100 real U.S. persons contacted through ORGANIZATION-controlled false U.S. persona accounts and tracked to monitor recruitment efforts and requests. The list included contact information for the U.S. persons, a summary of their political views, and activities they had been asked to perform by Defendants and their co-conspirators.

82. On or about August 31, 2016, Defendants and their co-conspirators, using a U.S. persona, spoke by telephone with a real U.S. person affiliated with a grassroots group in Florida. That individual requested assistance in organizing a rally in Miami, Florida. On or about September 9, 2016, Defendants and their co-conspirators sent the group an interstate wire to pay for materials needed for the Florida rally on or about September 11, 2016.

83. On or about August 31, 2016, Defendants and their co-conspirators created and purchased Facebook advertisements for a rally they organized and scheduled in New York for September 11, 2016.

84. On or about September 9, 2016, Defendants and their co-conspirators, through a false U.S. persona, contacted the real U.S. person who had impersonated Clinton at the West Palm Beach rally. Defendants and their co-conspirators sent that U.S. person money via interstate wire as an inducement to travel from Florida to New York and to dress in costume at another rally they organized.

85. On or about September 22, 2016, Defendants and their co-conspirators created and purchased Facebook advertisements for a series of rallies they organized in Pennsylvania called “Miners for Trump” and scheduled for October 2, 2016.

All in violation of Title 18, United States Code, Section 371.

COUNT TWO

(Conspiracy to Commit Wire Fraud and Bank Fraud)

86. Paragraphs 1 through 7, 9 through 27, and 29 through 85 of this Indictment are re-alleged and incorporated by reference as if fully set forth herein.

87. From in or around 2016 through present, in the District of Columbia and elsewhere, Defendants INTERNET RESEARCH AGENCY LLC, DZHEYKHUN NASIMI OGLY ASLANOV, and GLEB IGOREVICH VASILCHENKO, together with others known and unknown to the Grand Jury, knowingly and intentionally conspired to commit certain offenses against the United States, to wit:

- a. to knowingly, having devised and intending to devise a scheme and artifice to defraud, and to obtain money and property by means of false and fraudulent

pretenses, representations, and promises, transmit and cause to be transmitted, by means of wire communications in interstate and foreign commerce, writings, signs, signals, pictures, and sounds, for the purposes of executing such scheme and artifice, in violation of Title 18, United States Code, Section 1343; and

- b. to knowingly execute and attempt to execute a scheme and artifice to defraud a federally insured financial institution, and to obtain monies, funds, credits, assets, securities and other property from said financial institution by means of false and fraudulent pretenses, representations, and promises, all in violation of Title 18, United States Code, Section 1344.

Object of the Conspiracy

88. The conspiracy had as its object the opening of accounts under false names at U.S. financial institutions and a digital payments company in order to receive and send money into and out of the United States to support the ORGANIZATION's operations in the United States and for self-enrichment.

Manner and Means of the Conspiracy

89. Beginning in at least 2016, Defendants and their co-conspirators used, without lawful authority, the social security numbers, home addresses, and birth dates of real U.S. persons without their knowledge or consent. Using these means of stolen identification, Defendants and their co-conspirators opened accounts at a federally insured U.S. financial institution ("Bank 1"), including the following accounts:

Approximate Date	Account Name	Means of Identification
June 16, 2016	T.B.	Social Security Number Date of Birth
July 21, 2016	A.R.	Social Security Number Date of Birth
July 27, 2016	T.C.	Social Security Number Date of Birth
August 2, 2016	T.W.	Social Security Number Date of Birth

90. Defendants and their co-conspirators also used, without lawful authority, the social security numbers, home addresses, and birth dates of real U.S. persons to open accounts at PayPal, a digital payments company, including the following accounts:

Approximate Date	Initials of Identity Theft Victim	Means of Identification
June 16, 2016	T.B.	Social Security Number Date of Birth
July 21, 2016	A.R.	Social Security Number Date of Birth
August 2, 2016	T.W.	Social Security Number Date of Birth
November 11, 2016	J.W.	Home Address
January 18, 2017	V.S.	Social Security Number

Defendants and their co-conspirators also established other accounts at PayPal in the names of false and fictitious U.S. personas. Some personas used to register PayPal accounts were the same as the false U.S. personas used in connection with the ORGANIZATION's social media accounts.

91. Defendants and their co-conspirators purchased credit card and bank account numbers from online sellers for the unlawful purpose of evading security measures at PayPal, which used account numbers to verify a user's identity. Many of the bank account numbers purchased by Defendants

and their co-conspirators were created using the stolen identities of real U.S. persons. After purchasing the accounts, Defendants and their co-conspirators submitted these bank account numbers to PayPal.

92. On or about the dates identified below, Defendants and their co-conspirators obtained and used the following fraudulent bank account numbers for the purpose of evading PayPal's security measures:

Approximate Date	Card/Bank Account Number	Financial Institution	Email Used to Acquire Account Number
June 13, 2016	xxxxxxxx8902	Bank 2	wemakeweather@gmail.com
June 16, 2016	xxxxxxx8731	Bank 1	allforusa@yahoo.com
July 21, 2016	xxxxxxx2215	Bank 3	antwan_8@yahoo.com
August 2, 2016	xxxxxxx5707	Bank 1	xtimwaltersx@gmail.com
October 18, 2016	xxxxxxxxx5792	Bank 4	unitedvetsofamerica@gmail.com
October 18, 2016	xxxxxxxxx4743	Bank 4	patriototus@gmail.com
November 11, 2016	xxxxxxxxx2427	Bank 4	beautifullelly@gmail.com
November 11, 2016	xxxxxxxxx7587	Bank 5	staceyredneck@gmail.com
November 11, 2016	xxxxxxxxx7590	Bank 5	ihatecrime1@gmail.com
November 11, 2016	xxxxxxxxx1780	Bank 6	staceyredneck@gmail.com
November 11, 2016	xxxxxxxxx1762	Bank 6	ihatecrime1@gmail.com
December 13, 2016	xxxxxxxxx6168	Bank 6	thetaylorbrooks@aol.com
March 30, 2017	xxxxxxxxx6316	Bank 3	wokeaztec@outlook.com
March 30, 2017	xxxxxxx9512	Bank 3	wokeaztec@outlook.com

93. Additionally, and in order to maintain their accounts at PayPal and elsewhere, including online cryptocurrency exchanges, Defendants and their co-conspirators purchased and obtained false identification documents, including fake U.S. driver's licenses. Some false identification documents obtained by Defendants and their co-conspirators used the stolen identities of real U.S. persons, including U.S. persons T.W. and J.W.

94. After opening the accounts at Bank 1 and PayPal, Defendants and their co-conspirators used them to receive and send money for a variety of purposes, including to pay for certain ORGANIZATION expenses. Some PayPal accounts were used to purchase advertisements on Facebook promoting ORGANIZATION-controlled social media accounts. The accounts were also used to pay other ORGANIZATION-related expenses such as buttons, flags, and banners for rallies.

95. Defendants and their co-conspirators also used the accounts to receive money from real U.S. persons in exchange for posting promotions and advertisements on the ORGANIZATION-controlled social media pages. Defendants and their co-conspirators typically charged certain U.S. merchants and U.S. social media sites between 25 and 50 U.S. dollars per post for promotional content on their popular false U.S. persona accounts, including Being Patriotic, Defend the 2nd, and Blacktivist.

All in violation of Title 18, United States Code, Section 1349.

COUNTS THREE THROUGH EIGHT

(Aggravated Identity Theft)

96. Paragraphs 1 through 7, 9 through 27, and 29 through 85, and 89 through 95 of this Indictment are re-alleged and incorporated by reference as if fully set forth herein.

97. On or about the dates specified below, in the District of Columbia and elsewhere,

Defendants INTERNET RESEARCH AGENCY LLC, DZHEYKHUN NASIMI OGLY ASLANOV, GLEB IGOREVICH VASILCHENKO, IRINA VIKTOROVNA KAVERZINA, and VLADIMIR VENKOV did knowingly transfer, possess, and use, without lawful authority, a means of identification of another person during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c), to wit, wire fraud and bank fraud, knowing that the means of identification belonged to another real person:

Count	Approximate Date	Initials of Identity Theft Victim	Means of Identification
3	June 16, 2016	T.B.	Social Security Number Date of Birth
4	July 21, 2016	A.R.	Social Security Number Date of Birth
5	July 27, 2016	T.C.	Social Security Number Date of Birth
6	August 2, 2016	T.W.	Social Security Number Date of Birth
7	January 18, 2017	V.S.	Social Security Number
8	May 19, 2017	J.W.	Home Address Date of Birth

All in violation of Title 18, United States Code, Sections 1028A(a)(1) and 2.

FORFEITURE ALLEGATION

98. Pursuant to Federal Rule of Criminal Procedure 32.2, notice is hereby given to Defendants that the United States will seek forfeiture as part of any sentence in accordance with Title 18, United States Code, Sections 981(a)(1)(C) and 982(a)(2), and Title 28, United States Code, Section 2461(c), in the event of Defendants' convictions under Count Two of this Indictment. Upon conviction of the offense charged in Count Two, Defendants INTERNET RESEARCH AGENCY LLC, DZHEYKHUN NASIMI OGLY ASLANOV, and GLEB IGOREVICH VASILCHENKO

shall forfeit to the United States any property, real or personal, which constitutes or is derived from proceeds traceable to the offense of conviction. Upon conviction of the offenses charged in Counts Three through Eight, Defendants INTERNET RESEARCH AGENCY LLC, DZHEYKHUN NASIMI OGLY ASLANOV, GLEB IGOREVICH VASILCHENKO, IRINA VIKTOROVNA KAVERZINA, and VLADIMIR VENKOV shall forfeit to the United States any property, real or personal, which constitutes or is derived from proceeds traceable to the offense(s) of conviction. Notice is further given that, upon conviction, the United States intends to seek a judgment against each Defendant for a sum of money representing the property described in this paragraph, as applicable to each Defendant (to be offset by the forfeiture of any specific property).

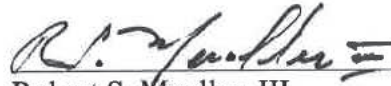
Substitute Assets

99. If any of the property described above as being subject to forfeiture, as a result of any act or omission of any defendant --

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third party;
- c. has been placed beyond the jurisdiction of the court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property that cannot be subdivided without difficulty;

it is the intent of the United States of America, pursuant to Title 18, United States Code, Section 982(b) and Title 28, United States Code, Section 2461(c), incorporating Title 21, United States Code, Section 853, to seek forfeiture of any other property of said Defendant.

(18 U.S.C. §§ 981(a)(1)(C) and 982; 28 U.S.C. § 2461(c))



Robert S. Mueller, III
Special Counsel
U.S. Department of Justice

A TRUE BILL:



Foreperson

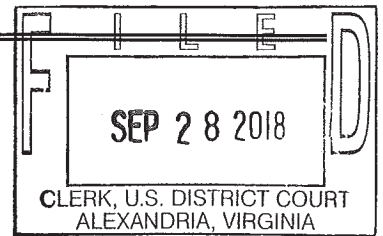
Date: February 16 2018

AO 91 (Rev. 11/11) Criminal Complaint

UNDER SEAL
UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia



United States of America

v.

Case No. 1:18-MJ-464

ELENA ALEKSEEVNA KHUSYAYNOVA

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of the year 2014 until the present in the county of Alexandria in the Eastern District of Virginia, the defendant(s) violated:

Code Section

Offense Description

18 U.S.C. § 371

Conspiracy to defraud the United States

This criminal complaint is based on these facts:

SEE ATTACHED AFFIDAVIT

☒ Continued on the attached sheet.

Reviewed by AUSA/SAUSA:

AUSA Jay Prabhu; SAUSA Alex Iftimie

David Holt
Complainant's signature

David Holt, Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: 28 Sep 18

City and state: Alexandria, Virginia

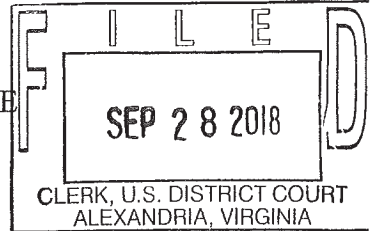
Ivan D. Davis /s/

Ivan D. Davis

United States Magistrate Judge

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division



UNITED STATES OF AMERICA

v.

ELENA ALEKSEEVNA KHUSYAYNOVA,

Defendant.

Case No. 1:18-MJ-464

18 U.S.C. § 371
(Conspiracy)

UNDER SEAL

AFFIDAVIT IN SUPPORT OF A CRIMINAL COMPLAINT

I, David Holt, being duly sworn under oath, do hereby depose and state:

INTRODUCTION

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been so employed since August 2008. I am presently assigned to the Washington Field Office where I am responsible for investigations of foreign influence operations and other national security matters with a cyber nexus. I have also conducted national security investigations of foreign intelligence services and the targeting of critical U.S. infrastructure. As a Special Agent, I have received specialized training and instruction in the field of national security investigations and am authorized to investigate violation of laws of the United States and to execute warrants issued under the authority of the United States.

2. I am submitting this affidavit in support of a criminal complaint and arrest warrant charging the defendant, ELENA ALEKSEEVNA KHUSYAYNOVA, with Conspiracy to defraud the United States, in violation of Title 18, United States Code, Section 371.

3. The statements contained in this Affidavit are based on my experience and background as a criminal investigator, on information provided to me by other members of the

FBI and other law enforcement officers, court records and documents, business records, interviews, publicly available information, and my review of physical and documentary evidence. I have personally participated in the investigation of the offense set forth below and, as a result of my participation and review of evidence gathered in the case, I am familiar with the facts and circumstances of this investigation. Since this Affidavit is being submitted for the limited purpose of supporting a criminal complaint, I have not included every fact resulting from the investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe the above-named defendant has violated Title 18, United States Code, Section 371, as set forth herein.

RELEVANT STATUTES AND BACKGROUND

4. Title 18, United States Code, Section 371, makes it a federal crime if “two or more persons conspire . . . to defraud the United States, or any agency thereof in any manner or for any purpose, and one or more of such persons do any act to effect the object of the conspiracy.”

5. The United States of America, through its departments and agencies, regulates the activities of foreign individuals and entities in and affecting the United States in order to prevent, disclose, and counteract improper foreign influence on U.S. elections and on the U.S. political system. U.S. law bans foreign nationals from making certain expenditures or providing things of value for the purpose of influencing federal elections. U.S. law also bars agents of any foreign entity from engaging in political activities within the United States without first registering with the Attorney General. Various federal agencies, including the U.S. Department of Justice and the Federal Election Commission, are charged with enforcing these laws.

6. The U.S. Department of Justice administers the Foreign Agent Registration Act (“FARA”), Title 22, United States Code, Section 611 *et seq.* FARA establishes a registration, reporting, and disclosure regime for agents of foreign principals (which includes foreign non-government individuals and entities) so that the U.S. government and the people of the United States are informed of the source of information and the identity of persons attempting to influence U.S. public opinion, policy, and law. FARA requires, among other things, that persons subject to its requirements submit periodic registration statements containing truthful information about their activities and the income earned from them. Disclosure of the required information allows the federal government and the American people to evaluate the statements and activities of such persons in light of their function as foreign agents.

7. The Federal Election Commission is a federal agency that administers the Federal Election Campaign Act (“FECA”). Among other things, FECA prohibits foreign nationals from making “a contribution or donation of money or other thing of value, or to make an express or implied promise to make a contribution or donation, in connection with a Federal, State, or local election.” 52 U.S.C. § 30121(a)(1)(A). FECA also requires that individuals or entities who make certain independent expenditures in federal elections report those expenditures to the Federal Election Commission. The reporting requirements permit the Federal Election Commission to fulfill its statutory duties of providing the American public with accurate data about the financial activities of individuals and entities supporting federal candidates, and enforcing FECA’s limits and prohibitions, including the ban on foreign expenditures.

STATEMENT OF PROBABLE CAUSE

I. Project Lakhta and Efforts to Interfere with U.S. Political System

8. Since at least 2014, known and unknown individuals, operating as part of a broader Russian effort known as “Project Lakhta,” have engaged in political and electoral interference operations targeting populations within the Russian Federation and in various other countries, including, but not limited to, the United States, members of the European Union, and Ukraine. Since at least May 2014, Project Lakhta’s stated goal in the United States was to spread distrust towards candidates for political office and the political system in general.

9. Beginning in or around mid-2014 and continuing to the present, Project Lakhta obscured its conduct by operating through a number of Russian entities, including Internet Research Agency LLC (“IRA”), Internet Research LLC, MediaSintez LLC, GlavSet LLC, MixInfo LLC, Azimut LLC, NovInfo LLC, Nevskiy News LLC (a/k/a “NevNov”), Economy Today LLC, National News LLC, Federal News Agency LLC (a/k/a “FAN”), and International News Agency LLC (a/k/a “MAN”). These entities employed hundreds of individuals in support of Project Lakhta’s operations with an annual global budget of millions of U.S. dollars. Only some of Project Lakhta’s activities were directed at the United States.

10. Concord Management and Consulting LLC and Concord Catering (collectively “Concord”) are related Russian entities with various Russian government contracts. Concord was the primary source of funding for Project Lakhta operations. Concord controlled funding, recommended personnel, and oversaw Project Lakhta activities through reporting and interaction with the management of the various Project Lakhta entities.

11. Yevgeniy Viktorovich Prigozhin is a Russian oligarch who is closely identified with Russian President Vladimir Putin. Prigozhin began his career in the food and restaurant

business and is sometimes referred to as “Putin’s Chef.” Prigozhin controls Concord, which has been paid by the Russian government to feed school children and the military. Concord and Prigozhin spent significant funds to further the Project Lakhta operations.

12. On February 16, 2018, a grand jury in the District of Columbia returned an indictment charging thirteen Russian nationals and three Russian companies, including Prigozhin, the IRA, and Concord, with committing federal crimes while seeking to interfere with U.S. elections and political processes, including the 2016 presidential election. Indictment, *United States v. Internet Research Agency, et al.*, 1:18-CR-32 (DLF) (D.D.C. Feb. 16, 2018). Based on my training and experience, the factual allegations in that indictment provide further probable cause to believe that the above-named defendant has violated Title 18, United States Code, Section 371. That indictment is attached hereto and incorporated by reference.

II. ELENA ALEKSEEVNA KHUSYAYNOVA

13. Defendant ELENA ALEKSEEVNA KHUSYAYNOVA is a resident of St. Petersburg, Russia. Since at least 2014, the defendant has been employed by various entities within Project Lakhta, including the IRA, GlavSet, and the Federal News Agency. Since approximately April 2014, she has acted as the Chief Accountant in Project Lakhta’s finance department. As detailed further herein, KHUSYAYNOVA oversaw all aspects of Project Lakhta financing. She managed the budgeting and payment of expenses associated with social media operations, web content, advertising campaigns, infrastructure, salaries, travel, office rent, furniture, and supplies, and the registration of legal entities used to further Project Lakhta activities.

14. There is probable cause to believe that, from at least 2014 to the present, KHUSYAYNOVA conspired with persons known and unknown to defraud the United States by

impairing, obstructing, and defeating the lawful functions of the U.S. Department of Justice and Federal Election Commission in administering federal requirements for disclosure of foreign involvement in certain domestic activities, in violation of Title 18, United States Code, Section 371. Among the persons with whom KHUSYAYNOVA conspired are known and unknown employees and associates of Concord and Project Lakhta entities. The Conspiracy had as its objects impairing, obstructing, and defeating the lawful governmental functions of the United States by dishonest means in order to enable Project Lakhta actors to interfere with U.S. political and electoral processes, including the 2018 U.S. elections.

III. Manner and Means of the Conspiracy

15. The Conspiracy has a strategic goal, which continues to this day, to sow division and discord in the U.S. political system, including by creating social and political polarization, undermining faith in democratic institutions, and influencing U.S. elections, including the upcoming 2018 midterm election. The Conspiracy has sought to conduct what it called internally “information warfare against the United States of America”¹ through fictitious U.S. personas on social media platforms and other Internet-based media.

16. Members of the Conspiracy, posing as U.S. persons, operated fictitious social media personas, pages, and groups designed to attract U.S. audiences and to address divisive U.S. political and social issues or advocate for the election or electoral defeat of particular candidates. These personas, groups, and pages falsely claimed to be controlled by U.S. activists when, in fact, they were controlled by members of the Conspiracy. Over time, these accounts

¹ Throughout this affidavit, statements by members of the Conspiracy are translated or quoted exactly as they appear in the source text, including any spelling, grammatical, or factual errors.

became the Conspiracy's primary means to reach significant numbers of Americans for purposes of interfering with the U.S. political system.

17. Members of the Conspiracy made various expenditures to carry out those activities, including buying social media analytics products and services, as well as advertisements on social media, in some instances through third-party intermediaries. Members of the Conspiracy also staged and promoted political rallies inside the United States, and while posing as U.S. grassroots entities and U.S. persons, and without revealing their Russian identities and Project Lakhta affiliation, promoted or disparaged candidates and campaigns and organized rallies and counter-protests around particular socially divisive issues.

A. KHUSYAYNOVA's Role in Project Lakhta

18. To effectively manage such a large-scale operation, the Conspiracy was headed by a management group and organized into departments, including a design and graphics department, an analysts department, a search-engine optimization ("SEO") department, an information-technology ("IT") department, and a finance department.

19. Between April 2014 and the present, KHUSYAYNOVA, as the Chief Accountant in Project Lakhta's finance department, managed the financing of substantially all aspects of Project operations, which included media and influence activities directed at the United States, the European Union, and Ukraine, as well as the Russian Federation. In that role, she oversaw the budgets of various Project Lakhta entities, including the IRA, MediaSintez LLC, GlavSet LLC, MixInfo LLC, Azimut LLC, NovInfo LLC, Nevskiy News LLC, Economy Today LLC, National News LLC, Federal News Agency LLC, and International News Agency LLC. KHUSYAYNOVA participated in the preparation and submission of hundreds of financial vouchers, budgets, and payment requests for the various Project Lakhta entities, often putting all

company names on the same paperwork and identifying them as part of Project Lakhta.

KHUSYAYNOVA maintained Project Lakhta monthly budgets and submitted associated requests for funds to the central finance offices of Concord, which were responsible for disbursing money to Project Lakhta entities.

20. To conceal the nature of Project Lakhta activities, since at least January 2016 the Conspiracy labeled the funds paid by Concord to Project Lakhta as payments related to software support and development. Moreover, since at least January 2016, Concord distributed funds to Project Lakhta through approximately fourteen bank accounts held in the names of Concord affiliates, including Glavnaya Liniya LLC, Mercuriy LLC, Obshchepit LLC, Potentsial LLC, RSP LLC, ASP LLC, MTTs LLC, Kompleksservis LLC, SPb Kulinariya LLC, Almira LLC, Pishchevik LLC, Galant LLC, Rayteks LLC, and Standart LLC. The Conspiracy described payments from these Concord entities to Project Lakhta as being in furtherance of a series of vague contracts that obscured or falsely stated the true intended use of the funds. At various times, such payments were described as being for “providing services to collect and process materials,” “providing services in developing an exporting module for results,” and “providing services for developing a statistical processing module” (preliminary translation of Russian text).

21. At the same time, KHUSYAYNOVA kept detailed financial documents that tracked itemized Project Lakhta expenses, including efforts to promote the illegal objects of the Conspiracy in the United States. For example, the financial documents included itemized budgets that included IT expenses, social media marketing expenses, and expenses for activities in the United States and the European Union, including expenditures for activists and advertisements on social media platforms. KHUSYAYNOVA also issued and kept track of requests to Concord for funds to cover those expenses. Between at least January 2016 and July

2018, these documents were updated and provided to Concord on approximately a monthly basis. The following illustrative examples demonstrate KHUSYAYNOVA's meticulous record-keeping and management of Project Lakhta funds:

- a. In or around January 2017, KHUSYAYNOVA compiled and submitted to Concord a planned itemized budget for February 2017 for Project Lakhta totaling approximately 60 million Russian rubles (approximately \$1 million U.S. dollars).² This budget also contained a backward-looking accounting of actual expenses for calendar year 2016, which totaled approximately 720 million Russian rubles (approximately \$12 million U.S. dollars). In addition to administrative expenses, such as office rent, utility payments, and garbage disposal, the budget identified IT expenses, such as "registration of domain names" and the purchase of "proxy servers;" and social media marketing expenses, such as expenses for "purchasing posts for social networks," "[a]dvertisement on Facebook," "[a]dvertisement on VKontakte," "[a]dvertisement on Instagram," "[p]romoting news postings on social networks," and social media optimization software (such as Twidium and Novapress) (preliminary translation of Russian text). The budgets also contained a section on "USA, EU" activities, which included itemized expenditures for "Instagram," "Facebook advertisement," and "Activists" (preliminary translation of Russian text). Moreover, the budgets identified expenditures for "bloggers" and "developing accounts" on Twitter, and for the development and promotion of online videos (preliminary translation of Russian text).

² For the purpose of this affidavit, the approximate U.S. dollar values are based on an approximate currency conversion rate of 60 Russian rubles to 1 U.S. dollar.

- b. To cover the February 2017 expenses, KHUSYAYNOVA requested funds from Concord in two parts. KHUSYAYNOVA requested approximately 25 million Russian rubles on or about February 16, 2017, and approximately 35 million Russian rubles on March 6, 2017.
- c. In or around January 2018, KHUSYAYNOVA compiled and submitted to Concord a planned itemized budget for February 2018 totaling approximately 100 million Russian rubles (approximately \$1.7 million U.S. dollars). This budget also contained a backward-looking accounting of actual expenses for calendar year 2017, which totaled approximately 733 million Russian rubles (approximately \$12.2 million U.S. dollars). The budget contained, among other things, all of the categories of itemized expenditures identified in subparagraph a, above.
- d. To cover substantial portions of the February 2018 expenses, KHUSYAYNOVA requested funds from Concord in at least six parts. KHUSYAYNOVA requested approximately 20 million Russian rubles on or about February 7, 2018, approximately 10 million Russian rubles on or about February 7, 2018, approximately 15 million Russian rubles on or about February 16, 2018, approximately 3 million Russian rubles on or about February 21, 2018, approximately 5 million Russian rubles on or about February 28, 2018, and approximately 31 million Russian rubles on or about March 6, 2018.
- e. In or around March 2018, KHUSYAYNOVA compiled and submitted to Concord a monthly budget for April 2018 for Project Lakhta that exceeded 107 million

Russian rubles (over \$1.75 million U.S. dollars). The budget contained, among other things, all of the itemized expenditures identified in subparagraph a, above.

- f. To cover substantial portions of the April 2018 expenses, KHUSYAYNOVA requested funds from Concord in at least two parts. KHUSYAYNOVA requested approximately 32 million Russian rubles on or about April 6, 2018, and approximately 21 million Russian rubles on or about May 8, 2018.
- g. In or around April 2018, KHUSYAYNOVA compiled and submitted to Concord a monthly budget for May 2018 for Project Lakhta that exceeded 111 million Russian rubles (over \$1.86 million U.S. dollars). The budget contained, among other things, all of the categories of itemized expenditures identified in subparagraph a, above.
- h. To cover substantial portions of the May 2018 expenses, she requested funds from Concord in at least three parts. She requested approximately 5 million Russian rubles on or about May 8, 2018, approximately 31 million Russian rubles on or about May 10, 2018, and approximately 35 million Russian rubles on or about June 9, 2018.
- i. On or about June 1, 2018, KHUSYAYNOVA compiled and submitted to Concord a monthly budget for June 2018 for Project Lakhta that exceeded 114 million Russian rubles (over \$1.9 million U.S. dollars). The budget contained, among other things, all of the categories of itemized expenditures identified in subparagraph a, above.
- j. To cover substantial portions of the June 2018 expenses, KHUSYAYNOVA requested funds from Concord in three parts. KHUSYAYNOVA requested

approximately 29 million Russian rubles on or about June 1, 2018, approximately 29 million Russian rubles on or about June 4, 2018, and approximately 36 million Russian rubles on July 10, 2018.

22. Between in or around January 2016 and in or around June 2018, Project Lakhta's proposed operating budget totaled more than 2 billion Russian rubles (over \$35 million U.S. dollars). Just between in or around January 2018 and in or around June 2018, Project Lakhta's proposed operating budget totaled more than 650 million Russian rubles (over \$10 million U.S. dollars).

23. KHUSYAYNOVA also monitored the Project Lakhta budget to ensure that expected payments from Concord were received. For example, on or about November 15, 2017, KHUSYAYNOVA contacted Concord to inform them that she had not received a payment from Almira LLC for certain Project Lakhta companies, and that she was urgently waiting for the payment. Similarly, on or about April 11, 2018, KHUSYAYNOVA confirmed to Concord that she had received payment for a portion of the March 2018 budget for Project Lakhta but was waiting for the remaining payment. On or about April 12, 2018, a Concord employee informed KHUSYAYNOVA that the remaining payment would be forthcoming.

24. Starting at least in or around 2015, the Conspiracy began to purchase advertisements on online social media sites to promote events and social media groups it controlled. These expenditures were included in the budgets that KHUSYAYNOVA submitted to Concord. For example, between approximately January 2018 and June 2018, KHUSYAYNOVA compiled and submitted to Concord expenditures of over 3.7 million Russian rubles (over \$60,000 U.S. dollars) for advertisements on Facebook and over 385,000 Russian rubles (over \$6,000 U.S. dollars) for advertisements on Instagram. Over that same timeframe,

the budget also included expenditures of over 1,100,000 Russian rubles (over \$18,000 U.S. dollars) for “bloggers” and “[d]eveloping accounts” on Twitter (preliminary translation of Russian text). Additionally, the budget included expenditures for “[r]enting software for social networks,” including payments for services to manage Twitter posts and generate additional followers (preliminary translation of Russian text).

B. Targeted Messaging to Sow Social and Political Discord

25. Between in or around December 2016 and in or around May 2018, as part of the Conspiracy’s effort to sow discord in the U.S. political system, members of the Conspiracy used social media and other internet platforms to inflame passions on a wide variety of topics, including immigration, gun control and the Second Amendment, the Confederate flag, race relations, LGBT issues, the Women’s March, and the NFL national anthem debate. Members of the Conspiracy took advantage of specific events in the United States to anchor their themes, including the shootings of church members in Charleston, South Carolina, and concert attendees in Las Vegas, Nevada; the Charlottesville “Unite the Right” rally and associated violence; police shootings of African-American men; as well as the personnel and policy decisions of the current U.S. administration.

26. Members of the Conspiracy were directed to create “political intensity through supporting radical groups, users dissatisfied with [the] social and economic situation and oppositional social movements.” The Conspiracy also sought, in the words of one member of the Conspiracy, to “effectively aggravate the conflict between minorities and the rest of the population.”

27. The Conspirators’ activities did not exclusively adopt one ideological viewpoint; they wrote on topics from varied and sometimes opposing perspectives. Members of the

Conspiracy also developed strategies and guidance to target audiences with conservative and liberal viewpoints, as well as particular social groups. For example, a member of the Conspiracy advised in or around October 2017 that “if you write posts in a liberal group, . . . you must not use Breitbart titles. On the contrary, if you write posts in a conservative group, do not use Washington Post or BuzzFeed’s titles.” Using the example of individuals of color who are also members of the lesbian, gay, bisexual, and transgender (“LGBT”) community, the member of the Conspiracy offered the following guidance on how to target the group:

Colored LGBT are less sophisticated than white; therefore, complicated phrases and messages do not work. Be careful dealing with racial content. Just like ordinary Blacks, Latinos, and Native Americans, colored LGBT people are very sensitive towards *#whiteprivilege* and they react to posts and pictures that favor white people. . . . Unlike with conservatives, infographics works well among LGBT and their liberal allies, and it does work very well. However, the content must be simple to understand consisting of short text in large font and a colorful picture. (Preliminary translation of Russian text.)

Members of the Conspiracy also sought to target the timing of their posts to attract the widest possible viewership. The same member of the Conspiracy referenced above offered the following guidance on how to overcome the time difference between Russia and the United States:

Posting can be problematic due to time difference, but if you make your re-posts in the morning St. Petersburg time, it works well with liberals – LGBT groups are often active at night. Also, the conservative can view your re-post when they wake up in the morning if you post it before you leave in the evening St. Petersburg time. (Preliminary translation of Russian text.)

28. Members of the Conspiracy also developed detailed analysis of timely news articles and guidance for how to describe the articles in social media posts in order to promote the objectives of the Conspiracy. For example, in or around early August 2017, one or more members of the Conspiracy working under the guise of the Facebook group “Secured Borders”

analyzed a large quantity of U.S. news articles, summarized the substance of the articles, and outlined ways for the conspiracy to promote them. Specifically, one or more members of the Conspiracy described each article and categorized its theme, provided a strategic response with a particular focus on how to target U.S. audiences, and then noted approval to use the strategic response. The strategic response was referred to as “Tasking Specifics,” which appeared to include an assignment to certain members of the Conspiracy to disseminate the message on social media platforms.

- a. Citing an online news article titled “McCain Says Thinking a Wall Will Stop Illegal Immigration is ‘Crazy,’” from on or about August 5, 2017, a member of the Conspiracy directed that the article be messaged in the following way:

Brand McCain as an old geezer who has lost it and who long ago belonged in a home for the elderly. Emphasize that John McCain’s pathological hatred towards Donald Trump and towards all his initiatives crosses all reasonable borders and limits. State that dishonorable scoundrels, such as McCain, immediately aim to destroy all the conservative voters’ hopes as soon as Trump tries to fulfill his election promises and tries to protect the American interests. (Preliminary translation of Russian text.)

- b. Citing an online news article titled “Paul Ryan Opposes Trump’s Immigration Cuts, Wants Struggling American Workers to Stay Poor,” from on or about August 5, 2017, a member of the Conspiracy directed that the article be messaged in the following way:

Brand Paul Ryan a complete and absolute nobody incapable of any decisiveness. Emphasize that while serving as Speaker, this two-faced loudmouth has not accomplished anything good for America or for American citizens. State that the only way to get rid of Ryan from Congress, provided he wins in the 2018 primaries, is to vote in favor of Randy Brice, an American veteran and an iron worker and a Democrat. (Preliminary translation of Russian text.)

- c. Citing an online news article titled “11 California Counties Might have More Registered Voters Than Eligible,” from on or about August 6, 2017, a member of the Conspiracy directed that the article be messaged in the following way:

In the California voter registration rolls, there are more registrants than there are residents. This is the time for American conservatives to sound the alarm before the elections turn the Constitution into a mockery and a celebration of lawlessness. Emphasize that previous falsifications during the U.S. elections used to be perceived as a myth; today they became a reality with a threatening force and are perceived accordingly. Emphasize that all illegal voters must be kept away from the ballot boxes at distances “beyond artillery firing range.” There is an urgent need to introduce voter IDs for all the states, above all in the blue (liberal and undecided) states. Remind that the majority of the “blue states” have no VOTER IDs, which suggests that large-scale falsifications are bound to be happening there. State in the end that the Democrats in the coming election will surely attempt to falsify the results. (Preliminary translation of Russian text.)

- d. Citing an online news article titled “Savage: Civil War if Trump Taken Down,” from on or about August 6, 2017, a member of the Conspiracy directed that the article be messaged in the following way:

Forcefully support Michael Savage’s point of view with competence and honesty. Savage made it clear that any attempt to remove Trump is a direct path to a civil war in the United States. Name those who oppose the president and those who impede his efforts to implement his pre-election promises. Focus on the fact that the Anti-Trump Republicans: a) drag their feet with regard to financing the construction of the border wall; b) are not lowering taxes; c) slander Trump and harm his reputation (bring up McCain); d) do not want to cancel Obamacare; e) are not in a hurry to adopt laws that oppose the refugees coming from Middle Eastern countries entering this country. Summarize that in case Republicans will not stop acting as traitors, they will bring upon themselves forces of civil retribution during the 2018 elections. (Preliminary translation of Russian text.)

- e. Citing an online news article titled “Trump: No Welfare To Migrants For Grants For First 5 Years” from on or about August 6, 2017, a member of the Conspiracy directed that the article be messaged in the following way:

Fully support Donald Trump and express the hope that this time around Congress will be forced to act as the president says it should. Emphasize that if Congress continues to act like the Colonial British government did before the War of Independence, this will call for another revolution. Summarize that Trump once again proved that he stands for protecting the interests of the United States of America. (Preliminary translation of Russian text.)

- f. Citing an online news article titled “The 8 Dirtiest Scandals of Robert Mueller No One Is Talking About,” from on or about August 7, 2017, a member of the Conspiracy directed that the article be messaged in the following way:

Special prosecutor Mueller is a puppet of the establishment. List scandals that took place when Mueller headed the FBI. Direct attention to the listed examples. State the following: It is a fact that the Special Prosecutor who leads the investigation against Trump represents the establishment: a politician with proven connections to the U.S. Democratic Party who says things that should either remove him from his position or disband the entire investigation commission. Summarize with a statement that Mueller is a very dependent and highly politicized figure; therefore, there will be no honest and open results from the investigation. Emphasize that the work of this commission is damaging to the country and is aimed to declare impeachment of Trump. Emphasize that it cannot be allowed, no matter what. (Preliminary translation of Russian text.)

- g. Citing an online news article titled “CNN’s Pro-Jeb! Republican: Trump White House Like a ‘Brothel,’” from on or about August 7, 2017, a member of the Conspiracy directed that the article be messaged in the following way:

CNN commentator “RINO” likened the Trump administration to a “brothel.” Mass News Media Criticism! Accuse CNN of yet another lie. State that during past elections, namely, this mainstream media, which supported Hillary Clinton’s candidacy

for U. S. President almost 100%, disseminated fake news, insulting statements, and lies about Donald Trump and his supporters. This continues now. This is precisely why such news sources as the New York Times, Washington Post, CNN, CBS, Time, and Huffington Post must not be taken seriously, for they are the main propaganda channels that are screwing with the heads of American citizens. Remind readers that each of the above-mentioned media resources supported Hillary Clinton and received funds from her election fund. They produced fake social study research results at polls predicting a Clinton win with a 10-15% lead over Trump and tried hard to insult and discredit Trump. Summarize with a statement that CNN long ago lost its reputation as a trusted source and that its reputation is still declining. (Preliminary translation of Russian text.)

- h. Citing an online news article titled “Pro-Amnesty Sen. Marco Rubio: Trump’s Immigration Bill Will Not Pass the Senate,” from on or about August 7, 2017, a member of the Conspiracy directed that the article be messaged in the following way:

VERY IMPORTANT! We expose Marco Rubio as a fake conservative who is a traitor to Republican values and who in his soul despises the American Constitution and civil liberties. Remind that Rubio is the protégé of the preposterous Jeb Bush, who is a disgrace to the conservative movement. State that victims of violence committed by illegals and the relatives of the victims hate Marco Rubio completely and wholeheartedly. In other words, Rubio is a liberal who penetrated the Republican Party for the purpose undermining it from the inside. Summarize in a statement that voting for Rubio during the Senate elections is practically the same as voting for Hillary Clinton. (Preliminary translation of Russian text.)

- i. Citing an online news article titled “Sanctuary City Objects to Arrest of Accused Illegal Alien Child Molester,” from on or about August 7, 2017, a member of the Conspiracy directed that the article be messaged in the following way:

Characterize the position of Californian sanctuary cities along with the position of the entire California administration as absolutely and completely treacherous and disgusting. Stress that protecting an illegal rapist who raped an American child is the peak of

wickedness and hypocrisy. Summarize in a statement that “sanctuary city” politicians should surrender their American citizenship, for they behave as true enemies of the United States of America. (Preliminary translation of Russian text.)

- j. Citing an online news article titled “Maryland City Mulling Over Idea to Let Illegal Immigrants Vote” from on or about August 7, 2017, a member of the Conspiracy directed that the article be messaged in the following way:

Stress that the leadership in sanctuary cities has lost all connection with reality and is trying to provide criminals who illegally crossed the U.S. borders with voting rights that are available only to the citizens of the United States. Summarize in a statement that the leaders of sanctuary cities are people without conscience and without any respect for the American Constitution. (Preliminary translation of Russian text.)

- k. Citing an online news article titled “Dobbs Slams McConnell, Says It’s Time to ‘Ditch Mitch,’” from on or about August 8, 2017, a member of the Conspiracy directed that the article be messaged in the following way:

It’s time for Mitch McConnell (leader of the Senate Republicans) to retire. Show solid support for the news anchor. Emphasize that McConnell exhausted himself as a politician. State that Mitch McConnell, like many other Republican senators, behaves as a renegade and a vile liberal. McConnell has done nothing to fulfill Trump’s and other Republicans’ election promises. Remind that McConnell is a friend of Joe Biden, who has no political principles. Emphasize that boycotting the conservative agenda is the most inadequate and treacherous behavior possible in the given situation. Summarize in a statement that people did not vote for the Republicans in 2014 and in 2016 so that today they would do the same things that Democrats usually busy themselves with. (Preliminary translation of Russian text.)

C. Use of Specific U.S. Fake Personas

29. Since at least in or around 2015, the Conspiracy used social media platforms to create thousands of social media and email accounts that appeared to be operated by U.S. persons and used them to create and amplify divisive social and political content targeting a U.S.

audience. These accounts were also used to advocate for the election or electoral defeat of particular candidates in the 2016 and 2018 U.S. elections, to post derogatory information about a number of candidates, and, on occasion, to promote political donations against particular candidates.

30. In or around May 2015, the Conspiracy created a Facebook account registered under the false U.S. persona “Helen Christopherson.” On her Facebook page, “Helen Christopherson” purported to be a resident of New York City and identified her hometown as Charleston, South Carolina. Between in or around March 2016 and in or around July 2017, while concealing its true identity, location, and purpose, the Conspiracy used the false U.S. persona “Helen Christopherson” to contact individuals and groups in the United States to promote protests, rallies, and marches, including by funding advertising, flyers, and rally supplies. Specific examples of this account’s activities, as well as the activities of other accounts described in this subsection, are contained in the Overt Acts section below.

31. In or around June 2015, the Conspiracy created a Facebook account registered under the false U.S. persona “Bertha Malone.” On her Facebook page, “Bertha Malone” purported to be a resident of New York City, identified her hometown as New York City, and stated that she had attended a university in New York City. In or around January 2016, the Conspiracy used the “Bertha Malone” Facebook account to create a Facebook page for a group called “Stop A.I.,” which is an abbreviation for “Stop All Invaders.” Between in or around December 2016 and in or around August 2017, while concealing its true identity, location, and purpose, the Conspiracy used the “Bertha Malone” Facebook account to create over 400 posts on Facebook containing inflammatory political and social content focused primarily on immigration and Islam. Between on or about July 17, 2017, and on or about July 23, 2017, alone, the content

on the “Stop A.I.” Facebook page reached approximately 1,385,795 individuals and approximately 130,851 individuals purposefully engaged with the Facebook page. In total, by on or about July 23, 2017, the Facebook page received approximately 194,221 total page likes.

32. The Conspiracy also used the “Bertha Malone” Facebook account, while concealing its true identity, location, and purpose, to solicit at least one person presumed to be located in the United States to assist with Project Lakhta’s social media activities in or around July 2017, such as by posting and managing content on the “Stop A.I.” Facebook page. Moreover, the Conspiracy used the “Stop A.I.” Facebook page to accept money from individuals to post ads and other content on the Facebook group’s page.

33. In or around June 2016, the Conspiracy created a Twitter account that went by various names, including “@UsaUsafortrump,” “@USAFordTrump,” “@TrumpWithUSA,” “@TrumpMov,” “@POTUSADJT,” “@imdeplorable201,” “@swampdrainer659,” “@maga2017trump,” and “@TXCowboysRawk.” Most recently, the Twitter account went by the name “@CovfefeNationUS.” Between in or around November 2017 and in or around December 2017, while concealing its true identity, location, and purpose, the Conspiracy used the Twitter account “@CovfefeNationUS” to post or repost over 23,000 messages.

34. In or around September 2016, the Conspiracy created a Facebook account registered under the false U.S. persona “Rachell Edison” and an associated Facebook page for a group called “Defend the 2nd.” Between in or around December 2016 and in or around May 2017, while concealing its true identity, location, and purpose, the Conspiracy used the “Rachell Edison” Facebook account to create over 700 posts on Facebook containing inflammatory political and social content primarily focused on gun control and the Second Amendment.

35. In or around March 2017, the Conspiracy created the Twitter account “@wokeluisa” registered under the false U.S. persona “Luisa Haynes.” Between in or around March 2017 and in or around March 2018, while concealing its true identity, location, and purpose, the Conspiracy used the Twitter account “@wokeluisa” to post over 2,000 Tweets on topics such as the 2018 midterm election, the disenfranchisement of African-American voters, the NFL national anthem debate, the current U.S. administration, and the U.S. President’s family. By in or around March 2018, the Twitter account amassed over 55,000 followers.

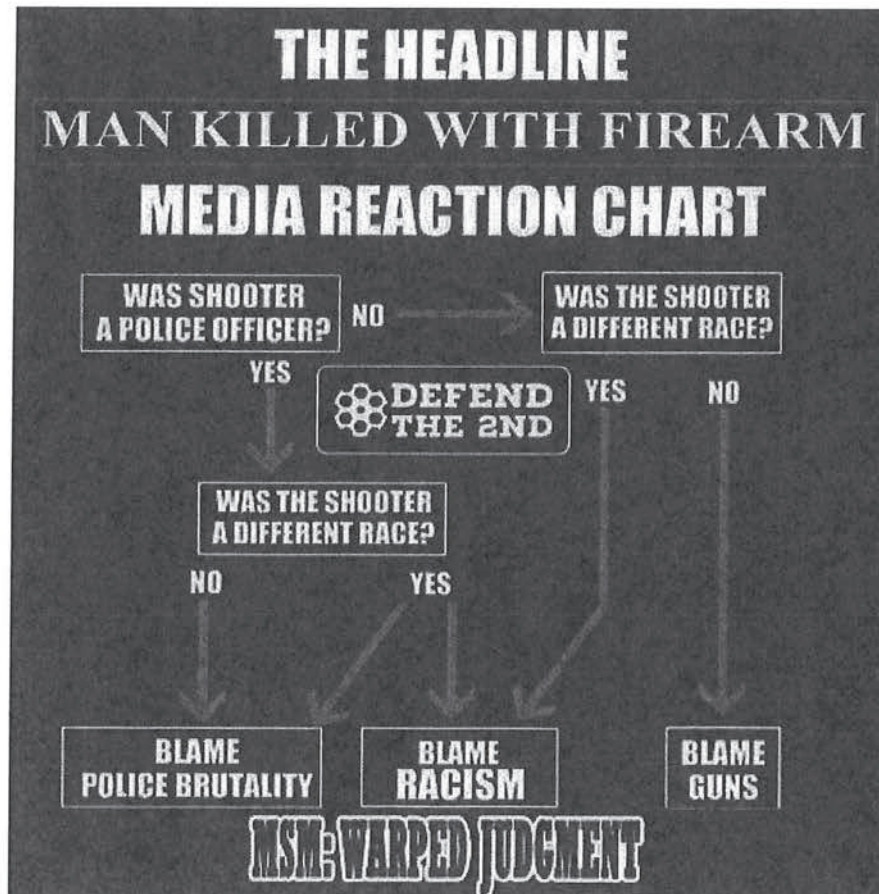
36. In or around September 2017, the Conspiracy created several Twitter accounts that it used to create and amplify content that would resonate with either liberal or conservative audiences. For example, on or about September 4, 2017, one or more members of the Conspiracy created the Twitter accounts “@JohnCopper16,” “@Amconvoice,” and “@TheTrainGuy13.” Members of the Conspiracy used these accounts to post messages on controversial social and political topics using a perspective that they believed would resonate with a conservative audience in the United States. Similarly, one or more members of the Conspiracy created the Twitter account “@KaniJJackson” on or about September 5, 2017, and the Twitter account “@JemiSHaaaZzz” on or about September 6, 2017, and used these accounts to post on many of the same controversial social and political topics from a perspective that they believed would resonate with a liberal audience in the United States. Between in or around September 2017 and in or around May 2018, while concealing its true identity, location, and purpose, the Conspiracy used these Twitter accounts to post thousands of Tweets, on topics including, but not limited to, the 2018 midterm election, gun rights, the net neutrality debate, negotiations with North Korea, and the personnel and policy decisions of the current U.S. administration. In some cases, these accounts attracted significant numbers of followers. For

example, by in or around May 2018, the Twitter account “@KaniJJackson” had amassed over 33,000 followers.

IV. Overt Acts

37. Between in or around December 2016 and in or around May 2018, in the Eastern District of Virginia and elsewhere, while concealing its true identity, location, and purpose, the Conspiracy committed the following overt acts involving U.S. social media platforms in furtherance of the Conspiracy and to effect its illegal objects:

38. On or about December 5, 2016, a member of the Conspiracy used the “Rachell Edison” Facebook account to post the following image on Facebook, accompanied by the comment “Whatever happens, blacks are innocent. Whatever happens, it’s all guns and cops. Whatever happens, it’s all racists and homophobes. MainStream Media...”:



39. On or about April 28, 2017, a member of the Conspiracy used the “Rachell Edison” Facebook account to post the following image on Facebook:



The image was accompanied by the following comment advocating political activities:

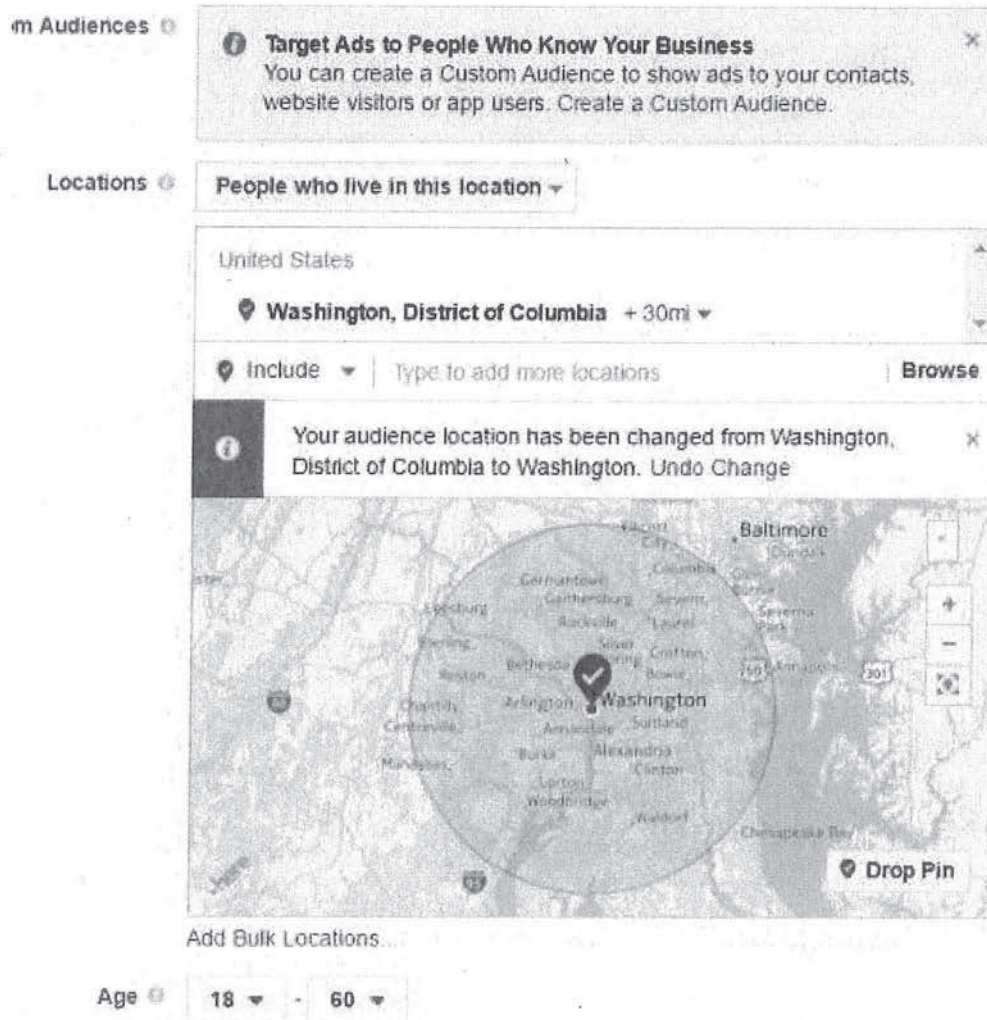
Gun rights backers need to make sure that election victories translate into action on Capitol Hill and expanded support in the states, the National Rifle Association’s legislative chief said Thursday, a day ahead of President Trump’s speech at the NRA’s annual convention. And he is absolutely right. Now it is the time for us to demand our rights. With current, administration it is possible to defend our right to bear arms. I think next 4 years will be great for all Americans, and for gun lovers especially! But we must stand for our rights! And in the end, I believe, we will win!

40. On or about July 1, 2017, a member of the Conspiracy used the “Helen Christopherson” Facebook account to contact the Facebook accounts for three real U.S. organizations (hereinafter U.S. Organizations 1, 2, and 3) to inquire about collaborating with

these groups on an anti-President Trump “flash mob” at the White House, which was already being organized by the groups for July 4, 2017. The organizers had described the event as “inviting resistance activists, show tune lovers, and karaoke fans to come join us on Independence Day, sing a song of freedom, and demand Trump’s impeachment.”

41. On or about July 2, 2017, a member of the Conspiracy used the “Helen Christopherson” Facebook account to contact U.S. Organization 1 and a U.S. person affiliated with the organization, U.S. Person 1, and inform them that “I got some cash on my Facebook ad account so we can promote it for 2 days,” adding “I got like \$80 on my ad account so we can reach like 10000 people in DC or so. That would be Massive!”

42. On or about July 2, 2017, a member of the Conspiracy used the “Helen Christopherson” Facebook account to send U.S. Organization 1 a proposal to purchase advertising targeting individuals within 30 miles of Washington, DC, including significant portions of the Eastern District of Virginia, as depicted below:



The proposed advertisements had an estimated reach of 29,000 to 58,000 individuals. Subsequently, U.S. Organization 1 agreed to make the “Helen Christopherson” Facebook account a co-organizer of the event on Facebook.

43. On or about July 4, 2017, a member of the Conspiracy used the “Bertha Malone” Facebook account to engage in the following conversation with U.S. Person 2 about U.S. Person 2 assisting with posting content and managing the “Stop A.I.” Facebook page, which members of the Conspiracy controlled:

Malone: Hey girl! How u doin? still got free time on ya hands?
So...remember u wanted to help me with that page i'm workng
on? It's a little bit unorthodox, but nwm that. Content is not of
my choosing. So what tell ya? Help a sister out?

U.S. Person 2: Hi! Let me think bout 4 a sec.
what's the name of the page again?

Malone: <https://www.facebook.com/StopAllInvaders/>

...

Malone: Nothin muh, [U.S. Person 2]. Just general scannin, answer
subscribers now and then and mb post something (i'll be sending
content to u directly)

Malone: nwm the posts lol

Malone: just business

Malone: makes ratinging for clients, that's what i know.

Malone: ratings*

Malone: u know how rednecks are

Malone: so here's the deal. I give u admin rights, u check the page when
i'm not around and basically do some stuff i tell u to :D

...

U.S. Person 2: You know I can't let my sis down

U.S. Person 2: so I'm in

...

U.S. Person 2: but please tell me I'm not going to jail for this

...

Malone: jeez why would u

Malone: just page lol

Malone: i'll vouch fou 4 mb u get some money out that even

...

U.S. Person 2: i trust you

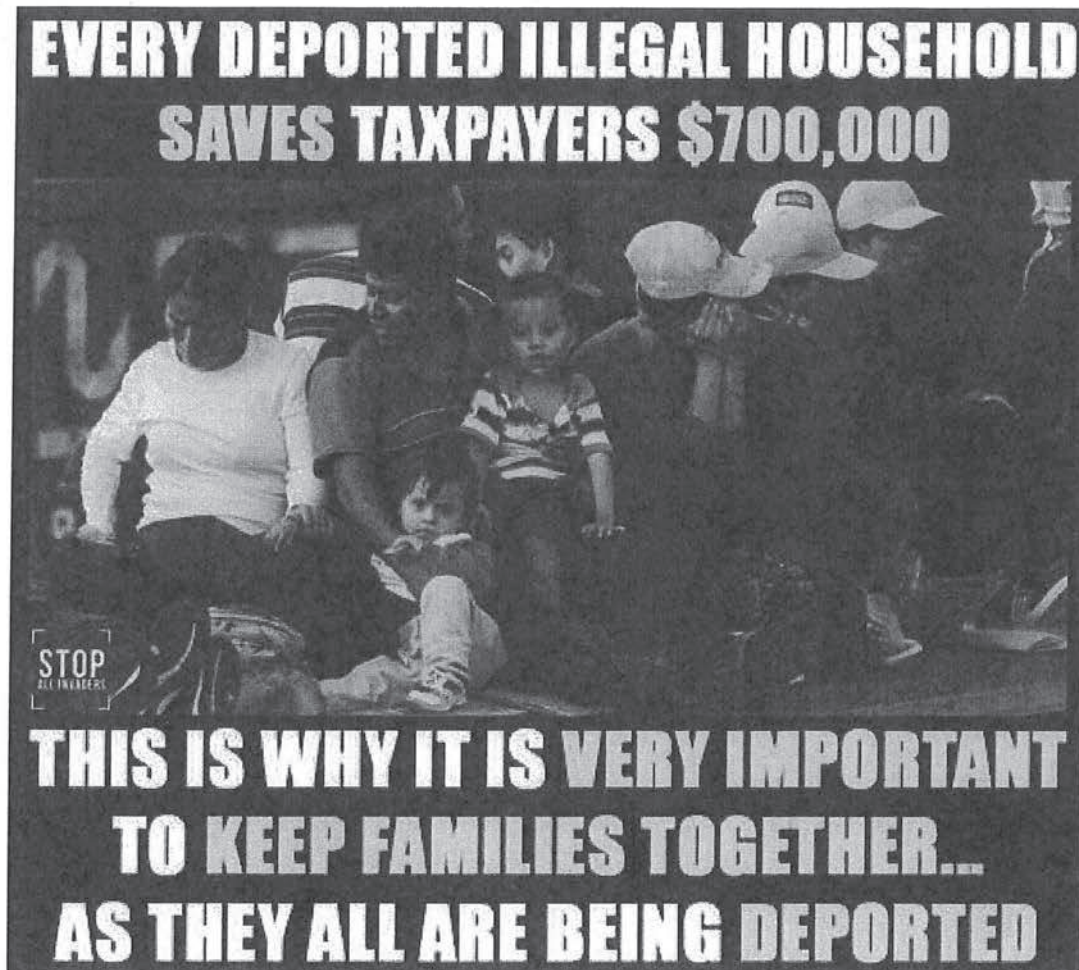
44. On or about July 28, 2017, a member of the Conspiracy used the “Bertha Malone” Facebook account to post the following image on Facebook:



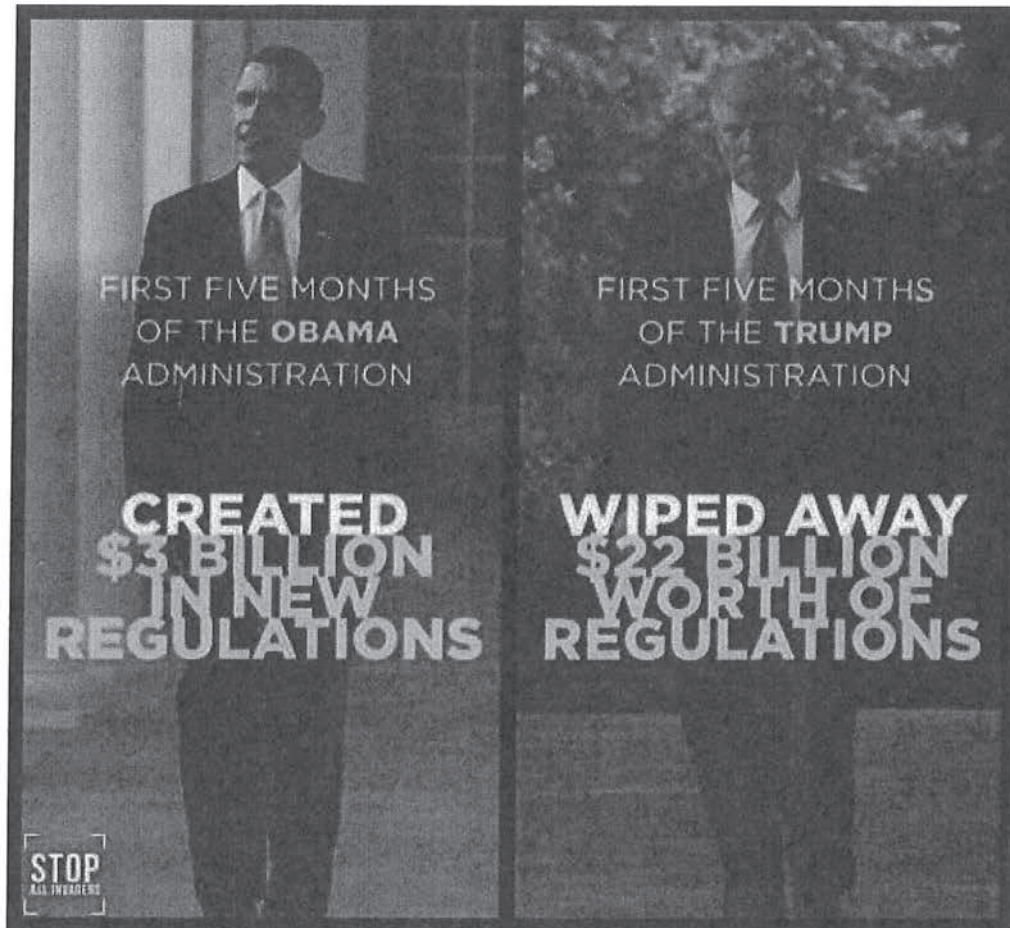
The image was accompanied by the following comment:

Instead this stupid witch hunt on Trump, media should investigate this traitor and his plan to Islamize our country. If you are true enemy of America, take a good look at Barack Hussein Obama and Muslim government officials appointed by him.

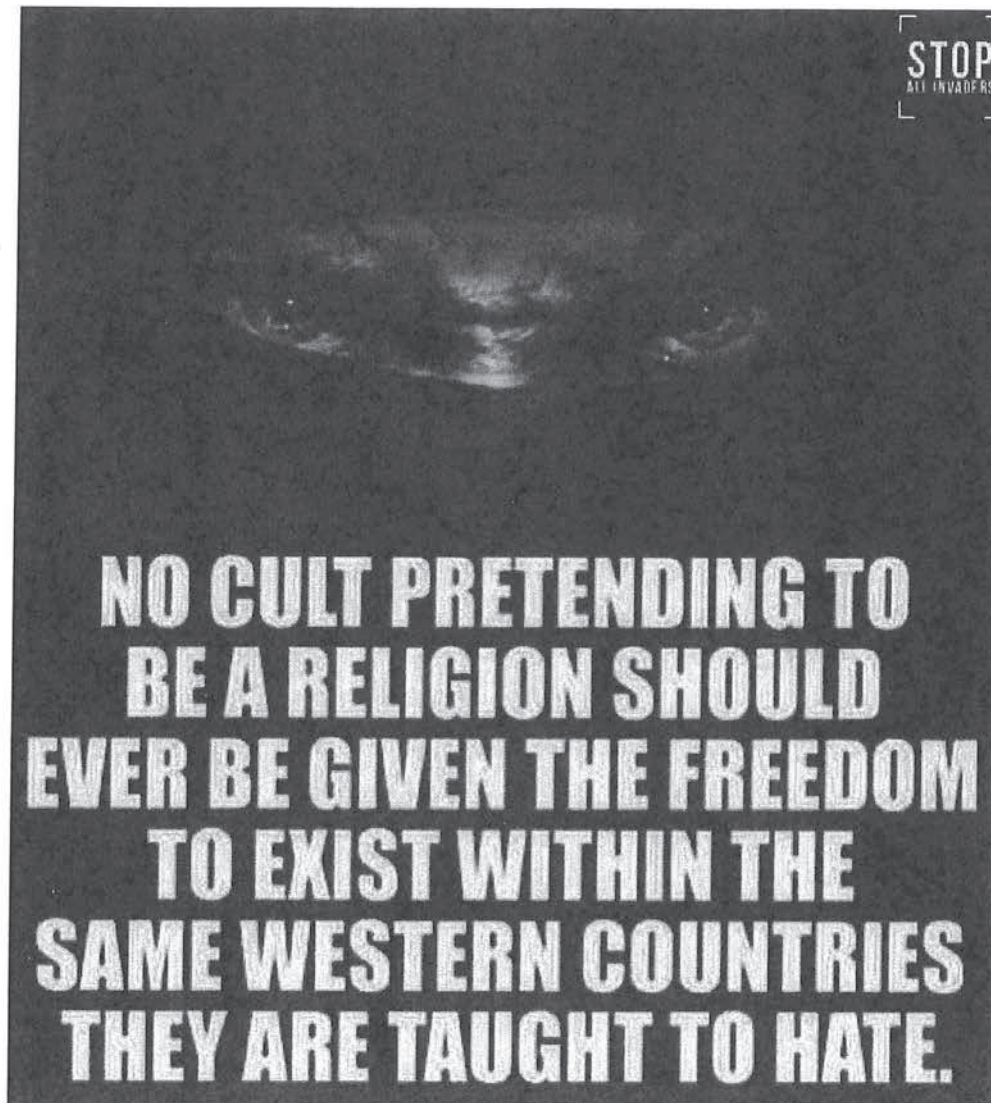
45. On or about July 31, 2017, a member of the Conspiracy used the “Bertha Malone” Facebook account to post the following image on Facebook, with the comment “Stop separating families! Deport them all, including their anchor babies! And spend saved money on Americans who really need it, for example our homeless Vets”:



46. On or about July 31, 2017, a member of the Conspiracy used the “Bertha Malone” Facebook account to post the following image on Facebook, with the comment “Feel the difference!”:



47. On or about August 1, 2017, a member of the Conspiracy used the “Bertha Malone” Facebook account to post the following image on Facebook, with the comment “Damn right! And we all know which cult we need to kick out of America...”:



The post generated approximately 104 comments between on or around August 1, 2017, and on or around August 2, 2017.

48. On or about December 10, 2017, a member of the Conspiracy used the Twitter account “@CovfefeNationUS” to repost a Tweet encouraging readers to donate to a political action committee aiming to unseat Democratic Senators and Representatives in the 2018 midterm election:

Tell us who you want to defeat! Donate \$1.00 to defeat @daveloebsack
Donate \$2.00 to defeat @SenatorBaldwin Donate \$3.00 to defeat
@clairecmc Donate \$4.00 to defeat @NancyPelosi Donate \$5.00 to defeat
@RepMaxineWaters Donate \$6.00 to defeat @SenWarren

The Tweet included a link to the donation website of a political action committee.

49. On or about December 12, 2017, a member of the Conspiracy used the Twitter account “@KaniJJackson” to post a Tweet about the 2017 special election in Alabama:

Dear Alabama, You have a choice today. Doug Jones put the KKK in prison for murdering 4 young black girls. Roy Moore wants to sleep with your teenage daughters. This isn't hard. #AlabamaSenate

50. On or about December 12, 2017, a member of the Conspiracy used the Twitter account “@JohnCopper16” to post a Tweet about the 2017 special election in Alabama:

People living in Alabama have different values than people living in NYC. They will vote for someone who represents them, for someone who they can trust. Not you. Dear Alabama, vote for Roy Moore.

51. On or about December 16, 2017, a member of the Conspiracy used the Twitter account “@KaniJJackson” to post a Tweet about the Special Counsel’s Office’s investigation:

If Trump fires Robert Mueller, we have to take to the streets in protest. Our democracy is at stake.

52. On or about December 17, 2017, a member of the Conspiracy used the Twitter account “@Amconvoice” to repost a Tweet about the Special Counsel’s Office’s investigation:

Liberals : If Trump fire/removes Mueller, we will take to the streets/protest. (DNC must have sent that talking point out today. Everyone using same line) Why would Trump need to remove/fire Mueller. Mueller is doing fine job destroying himself. Keep the implosion coming Mueller.

53. On or about January 19, 2018, a member of the Conspiracy used the Twitter account “@KaniJJackson” to post a Tweet about the government shutdown of 2018:


Who ended DACA? Who put off funding CHIP for 4 months? Who rejected a deal to restore DACA? It's not #SchumerShutdown. It's #GOPShutdown.

54. On or about January 20, 2018, a member of the Conspiracy used the Twitter account “@JohnCopper16” to repost a Tweet about the government shutdown of 2018:

Anyone who believes that President Trump is responsible for the #shutdown2018 is either an outright liar or horribly ignorant. #SchumerShutdown for illegals. #DemocratShutdown #DemocratLosers #DemocratsDefundMilitary #AlternativeFacts

55. On or about January 26, 2018, a member of the Conspiracy used the Twitter account “@JemiSHaaaZzz” to repost a Tweet about a Senate vote on reproductive health issues, referencing the telephone number of the U.S. Capitol switchboard:



Republicans have scheduled a vote Monday on legislation that would ban some women's health care choices 

We can't turn back the clock on women's reproductive health. Call your Senators now and tell them to vote NO: (202) 224-3121.

56. On or about February 8, 2018, a member of the Conspiracy used the Twitter account “@Amconvoice” to post a Tweet about the 2018 U.S. midterm election:

The only way the Democrats can win 101 GOP seats is to cheat like they always do with illegals & dead voters.

57. On or about February 15, 2018, a member of the Conspiracy used the Twitter account “@KaniJJackson” to post a Tweet about the Parkland, Florida, school shooting and the 2018 U.S. midterm election:

Reminder: the same GOP that is offering thoughts and prayers today are the same ones that voted to allow loosening gun laws for the mentally ill last February. If you're outraged today, VOTE THEM OUT IN 2018.
#guncontrol #Parkland

58. On or about February 16, 2018, a member of the Conspiracy used the Twitter account “@JemiSHaaaZzz” to repost a Tweet about the Special Counsel’s Office’s indictment of Russian companies and nationals who sought to interfere with U.S. elections and political processes:

Dear @realDonaldTrump: The DOJ indicted 13 Russian nationals at the Internet Research Agency for violating federal criminal law to help your campaign and hurt other campaigns. Still think this Russia thing is a hoax and a witch hunt? Because a lot of witches just got indicted.

59. On or about February 16, 2018, a member of the Conspiracy used the Twitter account “@JohnCopper16” to post two Tweets about the Special Counsel’s Office’s indictment:

Russians indicted today: 13 Illegal immigrants crossing Mexican border indicted today: 0 Anyway, I hope that all those Internet Research Agency f*ckers will be sent to gitmo.

We didn't vote for Trump because of a couple of hashtags shilled by the Russians. We voted for Trump because he convinced us to vote for Trump. And we are ready to vote for Trump again in 2020!

60. On or about February 19, 2018, a member of the Conspiracy used the Twitter account “@KaniJJackson” to post a Tweet about the 2018 midterm election:

Midterms are in 261 days, use this time to: - Promote your candidate on social media - Volunteer for a campaign - Donate to a campaign - Register to vote - Help others to register to vote - Spread the word We have only 261 days to guarantee survival of democracy. Get to work!

61. On or about February 27, 2018, a member of the Conspiracy used the Twitter account “@JohnCopper16” to post the following Tweet about the 2018 midterm election:

Dem 2018 platform: - We want women raped by the jihadists - We want children killed - We want higher gas prices - We want more illegal aliens - We want more Mexican drugs And they are wondering why @realDonaldTrump became the President...

62. On or about March 9, 2018, a member of the Conspiracy used the Twitter account “@JohnCopper16” to post the following two Tweets about the summit between President Trump and North Korean President Kim Jong Un:

WOW! Donald Trump is going to meet Kim Jong Un to discuss denuclearization of North Korea, If Trump gets North Korea to denuclearize its game over for the Democrats! That would be monumental!

RETWEET if you think that Donald Trump deserves a Nobel Peace Prize for resolving the North Korean crisis!

63. On or about March 9, 2018, a member of the Conspiracy used the Twitter account “@KaniJJackson” to post the following two Tweets about the summit between President Trump and North Korean President Kim Jong Un:

Trump says he will meet with Kim Jong Un in May. But he might not even be president by then. Mueller is coming!

The same people who criticized Barack Obama for signing the Iran Nuclear deal are already praising Trump for his promise to meet with Kim Jong Un and talk about denuclearization.

64. On or about March 14, 2018, a member of the Conspiracy used the Twitter account “@wokeluisa” to post several Tweets regarding the Pennsylvania special election on March 13, 2018, for a House of Representatives seat:

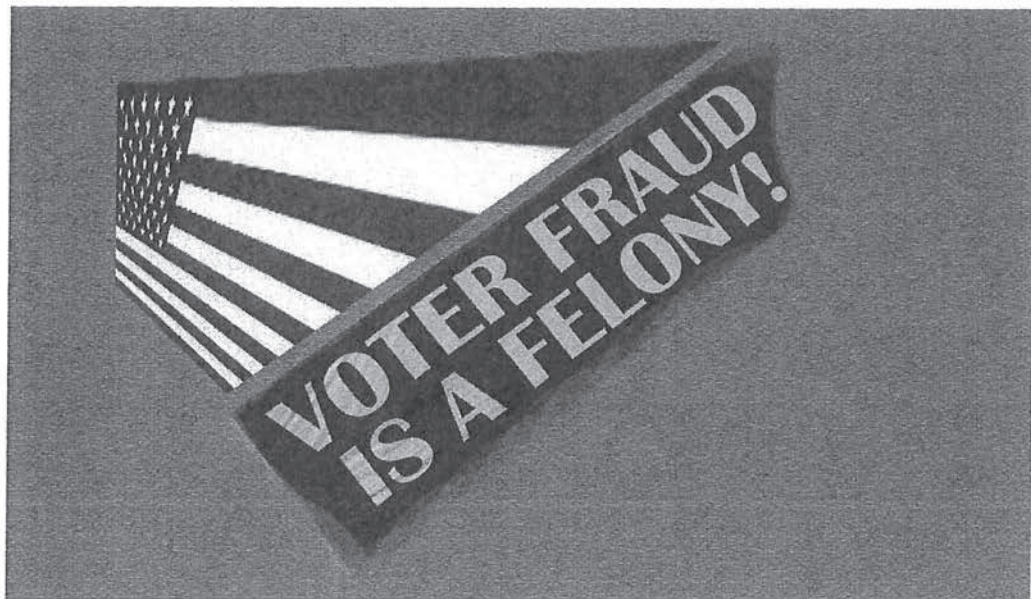
Enthusiastically watching #PA18 turn blue

Lamb up by only 703 votes... EVERY. VOTE. COUNTS. #PA18

We need to flip about 20 seats to regain control of the House! 19 after tonight! #PA18

Tonight's results are a message regardless of the outcome: D voters are motivated! Blue Wave coming! #PA18

65. On or about March 14, 2018, a member of the Conspiracy used the Twitter account "@TheTrainGuy13" to repost a Tweet about voter fraud:



66. On or about March 18, 2018, a member of the Conspiracy used the Twitter account “@wokeluisa” to post the following Tweet about election fraud:

Fun fact: the last time a new Republican president was elected without electoral fraud was in 1988

67. On or about March 18, 2018, a member of the Conspiracy used the Twitter account “@wokeluisa” to repost the following Tweet:

Just a reminder that: - Majority black Flint, Michigan still has drinking water that will give you brain damage if consumed. - Republicans are still trying to keep black people from voting. - A terrorist has been targeting black families for assassination in Austin, Texas.

68. On or about March 19, 2018, a member of the Conspiracy used the Twitter account “@wokeluisa” to post the following Tweets about an explosion in Austin, Texas:

Trump will tweet NOTHING about yet another explosion in Austin b/c all of the victims have been black and hispanic. Mark my words

Another explosion in southwest Austin, Texas! Why these bombings ain't a bigger story? Oh yes... all of the victims have been Black and Hispanic #AustinBombings

69. On or about March 19, 2018, a member of the Conspiracy used the Twitter account “@wokeluisa” to post the following Tweet about the 2018 midterm election:

Make sure to pre-register to vote if you are 16 y.o. or older. Don't just sit back, do something about everything that's going on because November 6, 2018 is the date that 33 senate seats, 435 seats in the House of Representatives and 36 governorships will be up for re-election.

70. On or about March 22, 2018, a member of the Conspiracy used the Twitter account “@johncopper16” to post the following Tweet about the 2018 midterm election:

Just a friendly reminder to get involved in the 2018 Midterms. They are motivated They hate you They hate your morals They hate your 1A and 2A rights They hate the Police They hate the Military They hate YOUR President

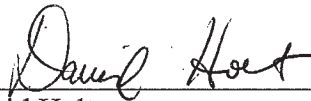
71. On or about May 17, 2018, a member of the Conspiracy used the Twitter account “@KaniJJackson” to repost two Tweets about a U.S. Senate vote on Net Neutrality:

Ted Cruz voted to repeal #NetNeutrality. Let’s save it and repeal him instead.

Here’s the list of GOP senators who broke party lines and voted to save #NetNeutrality: Susan Collins John N Kennedy Lisa Murkowski Thank you!

CONCLUSION

72. Based on the foregoing, and on my training, experience, and participation in this and other investigations, I submit there is probable cause to believe that, from at least 2014 to the present, ELENA ALEKSEEVNA KHUSYAYNOVA has violated Title 18, United States Code, Section 371.




David Holt
Special Agent
Federal Bureau of Investigation

Reviewed by:

Jay V. Prabhu
Chief, Cybercrime Unit
Assistant U.S. Attorney

Alex Iftimie
Special Assistant U.S. Attorney

Sworn to before me this 28 th day
of September, 2018

 /s/ _____
Ivan D. Davis
United States Magistrate Judge

UNITED STATES OF AMERICA

CRIMINAL NO.

(18 U.S.C. §§ 2, 371, 1030, 1028A, 1956, and 3551 et seq.)

Defendants.

* * * * *

The Grand Jury for the District of Columbia charges:

(Conspiracy to Commit an Offense Against the United States)

1. In or around 2016, the Russian Federation (“Russia”) operated a military intelligence agency called the Main Intelligence Directorate of the General Staff (“GRU”). The GRU had multiple units, including Units 26165 and 74455, engaged in cyber operations that involved the staged releases of documents stolen through computer intrusions. These units conducted large-scale cyber operations to interfere with the 2016 U.S. presidential election.

2. Defendants VIKTOR BORISOVICH NETYKSHO, BORIS ALEKSEYEVICH ANTONOV, DMITRIY SERGEYEVICH BADIN, IVAN SERGEYEVICH YERMAKOV, ALEKSEY VIKTOROVICH LUKASHEV, SERGEY ALEKSANDROVICH MORGACHEV, NIKOLAY YURYEVICH KOZACHEK, PAVEL VYACHESLAVOVICH YERSHOV, ARTEM ANDREYEVICH MALYSHEV, ALEKSANDR VLADIMIROVICH OSADCHUK, and ALEKSEY ALEKSANDROVICH POTEMKIN were GRU officers who knowingly and intentionally conspired with each other, and with persons known and unknown to the Grand Jury (collectively the “Conspirators”), to gain unauthorized access (to “hack”) into the computers of U.S. persons and entities involved in the 2016 U.S. presidential election, steal documents from those computers, and stage releases of the stolen documents to interfere with the 2016 U.S. presidential election.

3. Starting in at least March 2016, the Conspirators used a variety of means to hack the email accounts of volunteers and employees of the U.S. presidential campaign of Hillary Clinton (the “Clinton Campaign”), including the email account of the Clinton Campaign’s chairman.

4. By in or around April 2016, the Conspirators also hacked into the computer networks of the Democratic Congressional Campaign Committee (“DCCC”) and the Democratic National Committee (“DNC”). The Conspirators covertly monitored the computers of dozens of DCCC and DNC employees, implanted hundreds of files containing malicious computer code (“malware”), and stole emails and other documents from the DCCC and DNC.

5. By in or around April 2016, the Conspirators began to plan the release of materials stolen from the Clinton Campaign, DCCC, and DNC.

6. Beginning in or around June 2016, the Conspirators staged and released tens of thousands of the stolen emails and documents. They did so using fictitious online personas, including

“DCLeaks” and “Guccifer 2.0.”

7. The Conspirators also used the Guccifer 2.0 persona to release additional stolen documents through a website maintained by an organization (“Organization 1”), that had previously posted documents stolen from U.S. persons, entities, and the U.S. government. The Conspirators continued their U.S. election-interference operations through in or around November 2016.

8. To hide their connections to Russia and the Russian government, the Conspirators used false identities and made false statements about their identities. To further avoid detection, the Conspirators used a network of computers located across the world, including in the United States, and paid for this infrastructure using cryptocurrency.

Defendants

9. Defendant VIKTOR BORISOVICH NETYKSHO (НЕТЫКШО Виктор Борисович) was the Russian military officer in command of Unit 26165, located at 20 Komsomolskiy Prospekt, Moscow, Russia. Unit 26165 had primary responsibility for hacking the DCCC and DNC, as well as the email accounts of individuals affiliated with the Clinton Campaign.

10. Defendant BORIS ALEKSEYEVICH ANTONOV (Антонов Борис Алексеевич) was a Major in the Russian military assigned to Unit 26165. ANTONOV oversaw a department within Unit 26165 dedicated to targeting military, political, governmental, and non-governmental organizations with spearphishing emails and other computer intrusion activity. ANTONOV held the title “Head of Department.” In or around 2016, ANTONOV supervised other co-conspirators who targeted the DCCC, DNC, and individuals affiliated with the Clinton Campaign.

11. Defendant DMITRIY SERGEYEVICH BADIN (Бадин Дмитрий Сергеевич) was a Russian military officer assigned to Unit 26165 who held the title “Assistant Head of Department.” In or around 2016, BADIN, along with ANTONOV, supervised other co-conspirators who targeted the DCCC, DNC, and individuals affiliated with the Clinton Campaign.

12. Defendant IVAN SERGEYEVICH YERMAKOV (Ермаков Иван Сергеевич) was a Russian military officer assigned to ANTONOV's department within Unit 26165. Since in or around 2010, YERMAKOV used various online personas, including "Kate S. Milton," "James McMorgans," and "Karen W. Millen," to conduct hacking operations on behalf of Unit 26165. In or around March 2016, YERMAKOV participated in hacking at least two email accounts from which campaign-related documents were released through DCLeaks. In or around May 2016, YERMAKOV also participated in hacking the DNC email server and stealing DNC emails that were later released through Organization 1.

13. Defendant ALEKSEY VIKTOROVICH LUKASHEV (Лукашев Алексей Викторович) was a Senior Lieutenant in the Russian military assigned to ANTONOV's department within Unit 26165. LUKASHEV used various online personas, including "Den Katzenberg" and "Yuliana Martynova." In or around 2016, LUKASHEV sent spearphishing emails to members of the Clinton Campaign and affiliated individuals, including the chairman of the Clinton Campaign.

14. Defendant SERGEY ALEKSANDROVICH MORGACHEV (Моргачев Сергей Александрович) was a Lieutenant Colonel in the Russian military assigned to Unit 26165. MORGACHEV oversaw a department within Unit 26165 dedicated to developing and managing malware, including a hacking tool used by the GRU known as "X-Agent." During the hacking of the DCCC and DNC networks, MORGACHEV supervised the co-conspirators who developed and monitored the X-Agent malware implanted on those computers.

15. Defendant NIKOLAY YURYEVICH KOZACHEK (Козачек Николай Юрьевич) was a Lieutenant Captain in the Russian military assigned to MORGACHEV's department within Unit 26165. KOZACHEK used a variety of monikers, including "kazak" and "blablabla1234565." KOZACHEK developed, customized, and monitored X-Agent malware used to hack the DCCC

and DNC networks beginning in or around April 2016.

16. Defendant PAVEL VYACHESLAVOVICH YERSHOV (Ершов Павел Вячеславович) was a Russian military officer assigned to MORGACHEV's department within Unit 26165. In or around 2016, YERSHOV assisted KOZACHEK and other co-conspirators in testing and customizing X-Agent malware before actual deployment and use.

17. Defendant ARTEM ANDREYEVICH MALYSHEV (Малышев Артём Андреевич) was a Second Lieutenant in the Russian military assigned to MORGACHEV's department within Unit 26165. MALYSHEV used a variety of monikers, including "djangomagicdev" and "realblatr." In or around 2016, MALYSHEV monitored X-Agent malware implanted on the DCCC and DNC networks.

18. Defendant ALEKSANDR VLADIMIROVICH OSADCHUK (Осадчук Александр Владимирович) was a Colonel in the Russian military and the commanding officer of Unit 74455. Unit 74455 was located at 22 Kirova Street, Khimki, Moscow, a building referred to within the GRU as the "Tower." Unit 74455 assisted in the release of stolen documents through the DCLeaks and Guccifer 2.0 personas, the promotion of those releases, and the publication of anti-Clinton content on social media accounts operated by the GRU.

19. Defendant ALEKSEY ALEKSANDROVICH POTEKIN (Потемкин Алексей Александрович) was an officer in the Russian military assigned to Unit 74455. POTEKIN was a supervisor in a department within Unit 74455 responsible for the administration of computer infrastructure used in cyber operations. Infrastructure and social media accounts administered by POTEKIN's department were used, among other things, to assist in the release of stolen documents through the DCLeaks and Guccifer 2.0 personas.

Object of the Conspiracy

20. The object of the conspiracy was to hack into the computers of U.S. persons and entities involved in the 2016 U.S. presidential election, steal documents from those computers, and stage releases of the stolen documents to interfere with the 2016 U.S. presidential election.

Manner and Means of the Conspiracy

Spearphishing Operations

21. ANTONOV, BADIN, YERMAKOV, LUKASHEV, and their co-conspirators targeted victims using a technique known as spearphishing to steal victims' passwords or otherwise gain access to their computers. Beginning by at least March 2016, the Conspirators targeted over 300 individuals affiliated with the Clinton Campaign, DCCC, and DNC.

- a. For example, on or about March 19, 2016, LUKASHEV and his co-conspirators created and sent a spearphishing email to the chairman of the Clinton Campaign. LUKASHEV used the account "john356gh" at an online service that abbreviated lengthy website addresses (referred to as a "URL-shortening service"). LUKASHEV used the account to mask a link contained in the spearphishing email, which directed the recipient to a GRU-created website. LUKASHEV altered the appearance of the sender email address in order to make it look like the email was a security notification from Google (a technique known as "spoofing"), instructing the user to change his password by clicking the embedded link. Those instructions were followed. On or about March 21, 2016, LUKASHEV, YERMAKOV, and their co-conspirators stole the contents of the chairman's email account, which consisted of over 50,000 emails.
- b. Starting on or about March 19, 2016, LUKASHEV and his co-conspirators sent spearphishing emails to the personal accounts of other individuals affiliated with

the Clinton Campaign, including its campaign manager and a senior foreign policy advisor. On or about March 25, 2016, LUKASHEV used the same john356gh account to mask additional links included in spearphishing emails sent to numerous individuals affiliated with the Clinton Campaign, including Victims 1 and 2. LUKASHEV sent these emails from the Russia-based email account hi.mymail@yandex.com that he spoofed to appear to be from Google.

- c. On or about March 28, 2016, YERMAKOV researched the names of Victims 1 and 2 and their association with Clinton on various social media sites. Through their spearphishing operations, LUKASHEV, YERMAKOV, and their co-conspirators successfully stole email credentials and thousands of emails from numerous individuals affiliated with the Clinton Campaign. Many of these stolen emails, including those from Victims 1 and 2, were later released by the Conspirators through DCLeaks.
- d. On or about April 6, 2016, the Conspirators created an email account in the name (with a one-letter deviation from the actual spelling) of a known member of the Clinton Campaign. The Conspirators then used that account to send spearphishing emails to the work accounts of more than thirty different Clinton Campaign employees. In the spearphishing emails, LUKASHEV and his co-conspirators embedded a link purporting to direct the recipient to a document titled “hillary-clinton-favorable-rating.xlsx.” In fact, this link directed the recipients’ computers to a GRU-created website.

22. The Conspirators spearphished individuals affiliated with the Clinton Campaign throughout the summer of 2016. For example, on or about July 27, 2016, the Conspirators

attempted after hours to spearfish for the first time email accounts at a domain hosted by a third-party provider and used by Clinton's personal office. At or around the same time, they also targeted seventy-six email addresses at the domain for the Clinton Campaign.

Hacking into the DCCC Network

23. Beginning in or around March 2016, the Conspirators, in addition to their spearphishing efforts, researched the DCCC and DNC computer networks to identify technical specifications and vulnerabilities.

- a. For example, beginning on or about March 15, 2016, YERMAKOV ran a technical query for the DNC's internet protocol configurations to identify connected devices.
- b. On or about the same day, YERMAKOV searched for open-source information about the DNC network, the Democratic Party, and Hillary Clinton.
- c. On or about April 7, 2016, YERMAKOV ran a technical query for the DCCC's internet protocol configurations to identify connected devices.

24. By in or around April 2016, within days of YERMAKOV's searches regarding the DCCC, the Conspirators hacked into the DCCC computer network. Once they gained access, they installed and managed different types of malware to explore the DCCC network and steal data.

- a. On or about April 12, 2016, the Conspirators used the stolen credentials of a DCCC Employee ("DCCC Employee 1") to access the DCCC network. DCCC Employee 1 had received a spearphishing email from the Conspirators on or about April 6, 2016, and entered her password after clicking on the link.
- b. Between in or around April 2016 and June 2016, the Conspirators installed multiple versions of their X-Agent malware on at least ten DCCC computers, which allowed them to monitor individual employees' computer activity, steal passwords, and maintain access to the DCCC network.

- c. X-Agent malware implanted on the DCCC network transmitted information from the victims' computers to a GRU-leased server located in Arizona. The Conspirators referred to this server as their "AMS" panel. KOZACHEK, MALYSHEV, and their co-conspirators logged into the AMS panel to use X-Agent's keylog and screenshot functions in the course of monitoring and surveilling activity on the DCCC computers. The keylog function allowed the Conspirators to capture keystrokes entered by DCCC employees. The screenshot function allowed the Conspirators to take pictures of the DCCC employees' computer screens.
- d. For example, on or about April 14, 2016, the Conspirators repeatedly activated X-Agent's keylog and screenshot functions to surveil DCCC Employee 1's computer activity over the course of eight hours. During that time, the Conspirators captured DCCC Employee 1's communications with co-workers and the passwords she entered while working on fundraising and voter outreach projects. Similarly, on or about April 22, 2016, the Conspirators activated X-Agent's keylog and screenshot functions to capture the discussions of another DCCC Employee ("DCCC Employee 2") about the DCCC's finances, as well as her individual banking information and other personal topics.

25. On or about April 19, 2016, KOZACHEK, YERSHOV, and their co-conspirators remotely configured an overseas computer to relay communications between X-Agent malware and the AMS panel and then tested X-Agent's ability to connect to this computer. The Conspirators referred to this computer as a "middle server." The middle server acted as a proxy to obscure the connection between malware at the DCCC and the Conspirators' AMS panel. On or about April

20, 2016, the Conspirators directed X-Agent malware on the DCCC computers to connect to this middle server and receive directions from the Conspirators.

Hacking into the DNC Network

26. On or about April 18, 2016, the Conspirators hacked into the DNC's computers through their access to the DCCC network. The Conspirators then installed and managed different types of malware (as they did in the DCCC network) to explore the DNC network and steal documents.

- a. On or about April 18, 2016, the Conspirators activated X-Agent's keylog and screenshot functions to steal credentials of a DCCC employee who was authorized to access the DNC network. The Conspirators hacked into the DNC network from the DCCC network using stolen credentials. By in or around June 2016, they gained access to approximately thirty-three DNC computers.
- b. In or around April 2016, the Conspirators installed X-Agent malware on the DNC network, including the same versions installed on the DCCC network. MALYSHEV and his co-conspirators monitored the X-Agent malware from the AMS panel and captured data from the victim computers. The AMS panel collected thousands of keylog and screenshot results from the DCCC and DNC computers, such as a screenshot and keystroke capture of DCCC Employee 2 viewing the DCCC's online banking information.

Theft of DCCC and DNC Documents

27. The Conspirators searched for and identified computers within the DCCC and DNC networks that stored information related to the 2016 U.S. presidential election. For example, on or about April 15, 2016, the Conspirators searched one hacked DCCC computer for terms that included "hillary," "cruz," and "trump." The Conspirators also copied select DCCC folders, including "Benghazi Investigations." The Conspirators targeted computers containing information

such as opposition research and field operation plans for the 2016 elections.

28. To enable them to steal a large number of documents at once without detection, the Conspirators used a publicly available tool to gather and compress multiple documents on the DCCC and DNC networks. The Conspirators then used other GRU malware, known as “X-Tunnel,” to move the stolen documents outside the DCCC and DNC networks through encrypted channels.

- a. For example, on or about April 22, 2016, the Conspirators compressed gigabytes of data from DNC computers, including opposition research. The Conspirators later moved the compressed DNC data using X-Tunnel to a GRU-leased computer located in Illinois.
- b. On or about April 28, 2016, the Conspirators connected to and tested the same computer located in Illinois. Later that day, the Conspirators used X-Tunnel to connect to that computer to steal additional documents from the DCCC network.

29. Between on or about May 25, 2016 and June 1, 2016, the Conspirators hacked the DNC Microsoft Exchange Server and stole thousands of emails from the work accounts of DNC employees. During that time, YERMAKOV researched PowerShell commands related to accessing and managing the Microsoft Exchange Server.

30. On or about May 30, 2016, MALYSHEV accessed the AMS panel in order to upgrade custom AMS software on the server. That day, the AMS panel received updates from approximately thirteen different X-Agent malware implants on DCCC and DNC computers.

31. During the hacking of the DCCC and DNC networks, the Conspirators covered their tracks by intentionally deleting logs and computer files. For example, on or about May 13, 2016, the Conspirators cleared the event logs from a DNC computer. On or about June 20, 2016, the

Conspirators deleted logs from the AMS panel that documented their activities on the panel, including the login history.

Efforts to Remain on the DCCC and DNC Networks

32. Despite the Conspirators' efforts to hide their activity, beginning in or around May 2016, both the DCCC and DNC became aware that they had been hacked and hired a security company ("Company 1") to identify the extent of the intrusions. By in or around June 2016, Company 1 took steps to exclude intruders from the networks. Despite these efforts, a Linux-based version of X-Agent, programmed to communicate with the GRU-registered domain linuxknl.net, remained on the DNC network until in or around October 2016.

33. In response to Company 1's efforts, the Conspirators took countermeasures to maintain access to the DCCC and DNC networks.

- a. On or about May 31, 2016, YERMAKOV searched for open-source information about Company 1 and its reporting on X-Agent and X-Tunnel. On or about June 1, 2016, the Conspirators attempted to delete traces of their presence on the DCCC network using the computer program CCleaner.
- b. On or about June 14, 2016, the Conspirators registered the domain actblues.com, which mimicked the domain of a political fundraising platform that included a DCCC donations page. Shortly thereafter, the Conspirators used stolen DCCC credentials to modify the DCCC website and redirect visitors to the actblues.com domain.
- c. On or about June 20, 2016, after Company 1 had disabled X-Agent on the DCCC network, the Conspirators spent over seven hours unsuccessfully trying to connect to X-Agent. The Conspirators also tried to access the DCCC network using previously stolen credentials.

34. In or around September 2016, the Conspirators also successfully gained access to DNC computers hosted on a third-party cloud-computing service. These computers contained test applications related to the DNC's analytics. After conducting reconnaissance, the Conspirators gathered data by creating backups, or "snapshots," of the DNC's cloud-based systems using the cloud provider's own technology. The Conspirators then moved the snapshots to cloud-based accounts they had registered with the same service, thereby stealing the data from the DNC.

Stolen Documents Released through DCLeaks

35. More than a month before the release of any documents, the Conspirators constructed the online persona DCLeaks to release and publicize stolen election-related documents. On or about April 19, 2016, after attempting to register the domain electionleaks.com, the Conspirators registered the domain dcleaks.com through a service that anonymized the registrant. The funds used to pay for the dcleaks.com domain originated from an account at an online cryptocurrency service that the Conspirators also used to fund the lease of a virtual private server registered with the operational email account dirbinsaabol@mail.com. The dirbinsaabol email account was also used to register the john356gh URL-shortening account used by LUKASHEV to spearphish the Clinton Campaign chairman and other campaign-related individuals.

36. On or about June 8, 2016, the Conspirators launched the public website dcleaks.com, which they used to release stolen emails. Before it shut down in or around March 2017, the site received over one million page views. The Conspirators falsely claimed on the site that DCLeaks was started by a group of "American hacktivists," when in fact it was started by the Conspirators.

37. Starting in or around June 2016 and continuing through the 2016 U.S. presidential election, the Conspirators used DCLeaks to release emails stolen from individuals affiliated with the Clinton Campaign. The Conspirators also released documents they had stolen in other spearphishing operations, including those they had conducted in 2015 that collected emails from individuals

affiliated with the Republican Party.

38. On or about June 8, 2016, and at approximately the same time that the dcleaks.com website was launched, the Conspirators created a DCLeaks Facebook page using a preexisting social media account under the fictitious name “Alice Donovan.” In addition to the DCLeaks Facebook page, the Conspirators used other social media accounts in the names of fictitious U.S. persons such as “Jason Scott” and “Richard Gingrey” to promote the DCLeaks website. The Conspirators accessed these accounts from computers managed by POTEMKIN and his co-conspirators.

39. On or about June 8, 2016, the Conspirators created the Twitter account @dcleaks_. The Conspirators operated the @dcleaks_ Twitter account from the same computer used for other efforts to interfere with the 2016 U.S. presidential election. For example, the Conspirators used the same computer to operate the Twitter account @BaltimoreIsWhr, through which they encouraged U.S. audiences to “[j]oin our flash mob” opposing Clinton and to post images with the hashtag #BlacksAgainstHillary.

Stolen Documents Released through Guccifer 2.0

40. On or about June 14, 2016, the DNC—through Company 1—publicly announced that it had been hacked by Russian government actors. In response, the Conspirators created the online persona Guccifer 2.0 and falsely claimed to be a lone Romanian hacker to undermine the allegations of Russian responsibility for the intrusion.

41. On or about June 15, 2016, the Conspirators logged into a Moscow-based server used and managed by Unit 74455 and, between 4:19 PM and 4:56 PM Moscow Standard Time, searched for certain words and phrases, including:

Search Term(s)
“some hundred sheets”
“some hundreds of sheets”
dcleaks
illuminati
широко известный перевод [widely known translation]
“worldwide known”
“think twice about”
“company’s competence”

42. Later that day, at 7:02 PM Moscow Standard Time, the online persona Guccifer 2.0 published its first post on a blog site created through WordPress. Titled “DNC’s servers hacked by a lone hacker,” the post used numerous English words and phrases that the Conspirators had searched for earlier that day (bolded below):

Worldwide known cyber security company [Company 1] announced that the Democratic National Committee (DNC) servers had been hacked by “sophisticated” hacker groups.

I’m very pleased the company appreciated my skills so highly))) [. . .]

Here are just a few docs from many thousands I extracted when hacking into DNC’s network. [. . .]

Some hundred sheets! This’s a serious case, isn’t it? [. . .]

I guess [Company 1] customers should **think twice about company’s competence.**

F[***] the **Illuminati** and their conspiracies!!!!!!!!!! F[***]
[Company 1]!!!!!!!!!!

43. Between in or around June 2016 and October 2016, the Conspirators used Guccifer 2.0 to release documents through WordPress that they had stolen from the DCCC and DNC. The Conspirators, posing as Guccifer 2.0, also shared stolen documents with certain individuals.

a. On or about August 15, 2016, the Conspirators, posing as Guccifer 2.0, received a

request for stolen documents from a candidate for the U.S. Congress. The Conspirators responded using the Guccifer 2.0 persona and sent the candidate stolen documents related to the candidate's opponent.

- b. On or about August 22, 2016, the Conspirators, posing as Guccifer 2.0, transferred approximately 2.5 gigabytes of data stolen from the DCCC to a then-registered state lobbyist and online source of political news. The stolen data included donor records and personal identifying information for more than 2,000 Democratic donors.
- c. On or about August 22, 2016, the Conspirators, posing as Guccifer 2.0, sent a reporter stolen documents pertaining to the Black Lives Matter movement. The reporter responded by discussing when to release the documents and offering to write an article about their release.

44. The Conspirators, posing as Guccifer 2.0, also communicated with U.S. persons about the release of stolen documents. On or about August 15, 2016, the Conspirators, posing as Guccifer 2.0, wrote to a person who was in regular contact with senior members of the presidential campaign of Donald J. Trump, "thank u for writing back . . . do u find anyt[h]ing interesting in the docs i posted?" On or about August 17, 2016, the Conspirators added, "please tell me if i can help u anyhow . . . it would be a great pleasure to me." On or about September 9, 2016, the Conspirators, again posing as Guccifer 2.0, referred to a stolen DCCC document posted online and asked the person, "what do u think of the info on the turnout model for the democrats entire presidential campaign." The person responded, "[p]retty standard."

45. The Conspirators conducted operations as Guccifer 2.0 and DCLeaks using overlapping computer infrastructure and financing.

- a. For example, between on or about March 14, 2016 and April 28, 2016, the

Conspirators used the same pool of bitcoin funds to purchase a virtual private network (“VPN”) account and to lease a server in Malaysia. In or around June 2016, the Conspirators used the Malaysian server to host the dcleaks.com website. On or about July 6, 2016, the Conspirators used the VPN to log into the @Guccifer_2 Twitter account. The Conspirators opened that VPN account from the same server that was also used to register malicious domains for the hacking of the DCCC and DNC networks.

- b. On or about June 27, 2016, the Conspirators, posing as Guccifer 2.0, contacted a U.S. reporter with an offer to provide stolen emails from “Hillary Clinton’s staff.” The Conspirators then sent the reporter the password to access a nonpublic, password-protected portion of dcleaks.com containing emails stolen from Victim 1 by LUKASHEV, YERMAKOV, and their co-conspirators in or around March 2016.

46. On or about January 12, 2017, the Conspirators published a statement on the Guccifer 2.0 WordPress blog, falsely claiming that the intrusions and release of stolen documents had “totally no relation to the Russian government.”

Use of Organization 1

47. In order to expand their interference in the 2016 U.S. presidential election, the Conspirators transferred many of the documents they stole from the DNC and the chairman of the Clinton Campaign to Organization 1. The Conspirators, posing as Guccifer 2.0, discussed the release of the stolen documents and the timing of those releases with Organization 1 to heighten their impact on the 2016 U.S. presidential election.

- a. On or about June 22, 2016, Organization 1 sent a private message to Guccifer 2.0 to “[s]end any new material [stolen from the DNC] here for us to review and it will

have a much higher impact than what you are doing.” On or about July 6, 2016, Organization 1 added, “if you have anything hillary related we want it in the next tweeo [*sic*] days prefable [*sic*] because the DNC [Democratic National Convention] is approaching and she will solidify bernie supporters behind her after.” The Conspirators responded, “ok . . . i see.” Organization 1 explained, “we think trump has only a 25% chance of winning against hillary . . . so conflict between bernie and hillary is interesting.”

- b. After failed attempts to transfer the stolen documents starting in late June 2016, on or about July 14, 2016, the Conspirators, posing as Guccifer 2.0, sent Organization 1 an email with an attachment titled “wk dnc link1.txt.gpg.” The Conspirators explained to Organization 1 that the encrypted file contained instructions on how to access an online archive of stolen DNC documents. On or about July 18, 2016, Organization 1 confirmed it had “the 1Gb or so archive” and would make a release of the stolen documents “this week.”

48. On or about July 22, 2016, Organization 1 released over 20,000 emails and other documents stolen from the DNC network by the Conspirators. This release occurred approximately three days before the start of the Democratic National Convention. Organization 1 did not disclose Guccifer 2.0’s role in providing them. The latest-in-time email released through Organization 1 was dated on or about May 25, 2016, approximately the same day the Conspirators hacked the DNC Microsoft Exchange Server.

49. On or about October 7, 2016, Organization 1 released the first set of emails from the chairman of the Clinton Campaign that had been stolen by LUKASHEV and his co-conspirators. Between on or about October 7, 2016 and November 7, 2016, Organization 1 released

approximately thirty-three tranches of documents that had been stolen from the chairman of the Clinton Campaign. In total, over 50,000 stolen documents were released.

Statutory Allegations

50. Paragraphs 1 through 49 of this Indictment are re-alleged and incorporated by reference as if fully set forth herein.

51. From at least in or around March 2016 through November 2016, in the District of Columbia and elsewhere, Defendants NETYKSHO, ANTONOV, BADIN, YERMAKOV, LUKASHEV, MORGACHEV, KOZACHEK, YERSHOV, MALYSHEV, OSADCHUK, and POTEMKIN, together with others known and unknown to the Grand Jury, knowingly and intentionally conspired to commit offenses against the United States, namely:

- a. To knowingly access a computer without authorization and exceed authorized access to a computer, and to obtain thereby information from a protected computer, where the value of the information obtained exceeded \$5,000, in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and 1030(c)(2)(B); and
- b. To knowingly cause the transmission of a program, information, code, and command, and as a result of such conduct, to intentionally cause damage without authorization to a protected computer, and where the offense did cause and, if completed, would have caused, loss aggregating \$5,000 in value to at least one person during a one-year period from a related course of conduct affecting a protected computer, and damage affecting at least ten protected computers during a one-year period, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and 1030(c)(4)(B).

52. In furtherance of the Conspiracy and to effect its illegal objects, the Conspirators committed the overt acts set forth in paragraphs 1 through 19, 21 through 49, 55, and 57 through

64, which are re-alleged and incorporated by reference as if fully set forth herein.

53. In furtherance of the Conspiracy, and as set forth in paragraphs 1 through 19, 21 through 49, 55, and 57 through 64, the Conspirators knowingly falsely registered a domain name and knowingly used that domain name in the course of committing an offense, namely, the Conspirators registered domains, including dcleaks.com and actblues.com, with false names and addresses, and used those domains in the course of committing the felony offense charged in Count One.

All in violation of Title 18, United States Code, Sections 371 and 3559(g)(1).

COUNTS TWO THROUGH NINE
(Aggravated Identity Theft)

54. Paragraphs 1 through 19, 21 through 49, and 57 through 64 of this Indictment are re-alleged and incorporated by reference as if fully set forth herein.

55. On or about the dates specified below, in the District of Columbia and elsewhere, Defendants VIKTOR BORISOVICH NETYKSHO, BORIS ALEKSEYEVICH ANTONOV, DMITRIY SERGEYEVICH BADIN, IVAN SERGEYEVICH YERMAKOV, ALEKSEY VIKTOROVICH LUKASHEV, SERGEY ALEKSANDROVICH MORGACHEV, NIKOLAY YURYEVICH KOZACHEK, PAVEL VYACHESLAVOVICH YERSHOV, ARTEM ANDREYEVICH MALYSHEV, ALEKSANDR VLADIMIROVICH OSADCHUK, and ALEKSEY ALEKSANDROVICH POTEMKIN did knowingly transfer, possess, and use, without lawful authority, a means of identification of another person during and in relation to a felony violation enumerated in Title 18, United States Code, Section 1028A(c), namely, computer fraud in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and 1030(c)(2)(B), knowing that the means of identification belonged to another real person:

Count	Approximate Date	Victim	Means of Identification
2	March 21, 2016	Victim 3	Username and password for personal email account
3	March 25, 2016	Victim 1	Username and password for personal email account
4	April 12, 2016	Victim 4	Username and password for DCCC computer network
5	April 15, 2016	Victim 5	Username and password for DCCC computer network
6	April 18, 2016	Victim 6	Username and password for DCCC computer network
7	May 10, 2016	Victim 7	Username and password for DNC computer network
8	June 2, 2016	Victim 2	Username and password for personal email account
9	July 6, 2016	Victim 8	Username and password for personal email account

All in violation of Title 18, United States Code, Sections 1028A(a)(1) and 2.

COUNT TEN
(Conspiracy to Launder Money)

56. Paragraphs 1 through 19, 21 through 49, and 55 are re-alleged and incorporated by reference as if fully set forth herein.

57. To facilitate the purchase of infrastructure used in their hacking activity—including hacking into the computers of U.S. persons and entities involved in the 2016 U.S. presidential election and releasing the stolen documents—the Defendants conspired to launder the equivalent of more than \$95,000 through a web of transactions structured to capitalize on the perceived anonymity of cryptocurrencies such as bitcoin.

58. Although the Conspirators caused transactions to be conducted in a variety of currencies, including U.S. dollars, they principally used bitcoin when purchasing servers, registering domains, and otherwise making payments in furtherance of hacking activity. Many of these payments were

processed by companies located in the United States that provided payment processing services to hosting companies, domain registrars, and other vendors both international and domestic. The use of bitcoin allowed the Conspirators to avoid direct relationships with traditional financial institutions, allowing them to evade greater scrutiny of their identities and sources of funds.

59. All bitcoin transactions are added to a public ledger called the Blockchain, but the Blockchain identifies the parties to each transaction only by alpha-numeric identifiers known as bitcoin addresses. To further avoid creating a centralized paper trail of all of their purchases, the Conspirators purchased infrastructure using hundreds of different email accounts, in some cases using a new account for each purchase. The Conspirators used fictitious names and addresses in order to obscure their identities and their links to Russia and the Russian government. For example, the dcleaks.com domain was registered and paid for using the fictitious name “Carrie Feehan” and an address in New York. In some cases, as part of the payment process, the Conspirators provided vendors with nonsensical addresses such as “usa Denver AZ,” “ghfgh ghfhgh fdgfdg WA,” and “1 2 dwd District of Columbia.”

60. The Conspirators used several dedicated email accounts to track basic bitcoin transaction information and to facilitate bitcoin payments to vendors. One of these dedicated accounts, registered with the username “gfadel47,” received hundreds of bitcoin payment requests from approximately 100 different email accounts. For example, on or about February 1, 2016, the gfadel47 account received the instruction to “[p]lease send *exactly* **0.026043** bitcoin to” a certain thirty-four character bitcoin address. Shortly thereafter, a transaction matching those exact instructions was added to the Blockchain.

61. On occasion, the Conspirators facilitated bitcoin payments using the same computers that they used to conduct their hacking activity, including to create and send test spearphishing emails.

Additionally, one of these dedicated accounts was used by the Conspirators in or around 2015 to renew the registration of a domain (linuxkrnl.net) encoded in certain X-Agent malware installed on the DNC network.

62. The Conspirators funded the purchase of computer infrastructure for their hacking activity in part by “mining” bitcoin. Individuals and entities can mine bitcoin by allowing their computing power to be used to verify and record payments on the bitcoin public ledger, a service for which they are rewarded with freshly-minted bitcoin. The pool of bitcoin generated from the GRU’s mining activity was used, for example, to pay a Romanian company to register the domain dcleaks.com through a payment processing company located in the United States.

63. In addition to mining bitcoin, the Conspirators acquired bitcoin through a variety of means designed to obscure the origin of the funds. This included purchasing bitcoin through peer-to-peer exchanges, moving funds through other digital currencies, and using pre-paid cards. They also enlisted the assistance of one or more third-party exchangers who facilitated layered transactions through digital currency exchange platforms providing heightened anonymity.

64. The Conspirators used the same funding structure—and in some cases, the very same pool of funds—to purchase key accounts, servers, and domains used in their election-related hacking activity.

- a. The bitcoin mining operation that funded the registration payment for dcleaks.com also sent newly-minted bitcoin to a bitcoin address controlled by “Daniel Farrell,” the persona that was used to renew the domain linuxkrnl.net. The bitcoin mining operation also funded, through the same bitcoin address, the purchase of servers and domains used in the GRU’s spearphishing operations, including accounts-qooqle.com and account-goooogle.com.

- b. On or about March 14, 2016, using funds in a bitcoin address, the Conspirators purchased a VPN account, which they later used to log into the @Guccifer_2 Twitter account. The remaining funds from that bitcoin address were then used on or about April 28, 2016, to lease a Malaysian server that hosted the dcleaks.com website.
- c. The Conspirators used a different set of fictitious names (including “Ward DeClaus” and “Mike Long”) to send bitcoin to a U.S. company in order to lease a server used to administer X-Tunnel malware implanted on the DCCC and DNC networks, and to lease two servers used to hack the DNC’s cloud network.

Statutory Allegations

65. From at least in or around 2015 through 2016, within the District of Columbia and elsewhere, Defendants VIKTOR BORISOVICH NETYKSHO, BORIS ALEKSEYEVICH ANTONOV, DMITRIY SERGEYEVICH BADIN, IVAN SERGEYEVICH YERMAKOV, ALEKSEY VIKTOROVICH LUKASHEV, SERGEY ALEKSANDROVICH MORGACHEV, NIKOLAY YURYEVICH KOZACHEK, PAVEL VYACHESLAVOVICH YERSHOV, ARTEM ANDREYEVICH MALYSHEV, ALEKSANDR VLADIMIROVICH OSADCHUK, and ALEKSEY ALEKSANDROVICH POTEMKIN, together with others, known and unknown to the Grand Jury, did knowingly and intentionally conspire to transport, transmit, and transfer monetary instruments and funds to a place in the United States from and through a place outside the United States and from a place in the United States to and through a place outside the United States, with the intent to promote the carrying on of specified unlawful activity, namely, a violation of Title 18, United States Code, Section 1030, contrary to Title 18, United States Code, Section 1956(a)(2)(A).

All in violation of Title 18, United States Code, Section 1956(h).

COUNT ELEVEN

(Conspiracy to Commit an Offense Against the United States)

66. Paragraphs 1 through 8 of this Indictment are re-alleged and incorporated by reference as if fully set forth herein.

Defendants

67. Paragraph 18 of this Indictment relating to ALEKSANDR VLADIMIROVICH OSADCHUK is re-alleged and incorporated by reference as if fully set forth herein.

68. Defendant ANATOLIY SERGEYEVICH KOVALEV (Ковалев Анатолий Сергеевич) was an officer in the Russian military assigned to Unit 74455 who worked in the GRU's 22 Kirova Street building (the Tower).

69. Defendants OSADCHUK and KOVALEV were GRU officers who knowingly and intentionally conspired with each other and with persons, known and unknown to the Grand Jury, to hack into the computers of U.S. persons and entities responsible for the administration of 2016 U.S. elections, such as state boards of elections, secretaries of state, and U.S. companies that supplied software and other technology related to the administration of U.S. elections.

Object of the Conspiracy

70. The object of the conspiracy was to hack into protected computers of persons and entities charged with the administration of the 2016 U.S. elections in order to access those computers and steal voter data and other information stored on those computers.

Manner and Means of the Conspiracy

71. In or around June 2016, KOVALEV and his co-conspirators researched domains used by U.S. state boards of elections, secretaries of state, and other election-related entities for website vulnerabilities. KOVALEV and his co-conspirators also searched for state political party email addresses, including filtered queries for email addresses listed on state Republican Party websites.

72. In or around July 2016, KOVALEV and his co-conspirators hacked the website of a state board of elections (“SBOE 1”) and stole information related to approximately 500,000 voters, including names, addresses, partial social security numbers, dates of birth, and driver’s license numbers.

73. In or around August 2016, KOVALEV and his co-conspirators hacked into the computers of a U.S. vendor (“Vendor 1”) that supplied software used to verify voter registration information for the 2016 U.S. elections. KOVALEV and his co-conspirators used some of the same infrastructure to hack into Vendor 1 that they had used to hack into SBOE 1.

74. In or around August 2016, the Federal Bureau of Investigation issued an alert about the hacking of SBOE 1 and identified some of the infrastructure that was used to conduct the hacking. In response, KOVALEV deleted his search history. KOVALEV and his co-conspirators also deleted records from accounts used in their operations targeting state boards of elections and similar election-related entities.

75. In or around October 2016, KOVALEV and his co-conspirators further targeted state and county offices responsible for administering the 2016 U.S. elections. For example, on or about October 28, 2016, KOVALEV and his co-conspirators visited the websites of certain counties in Georgia, Iowa, and Florida to identify vulnerabilities.

76. In or around November 2016 and prior to the 2016 U.S. presidential election, KOVALEV and his co-conspirators used an email account designed to look like a Vendor 1 email address to send over 100 spearphishing emails to organizations and personnel involved in administering elections in numerous Florida counties. The spearphishing emails contained malware that the Conspirators embedded into Word documents bearing Vendor 1’s logo.

Statutory Allegations

77. Between in or around June 2016 and November 2016, in the District of Columbia and

elsewhere, Defendants OSADCHUK and KOVALEV, together with others known and unknown to the Grand Jury, knowingly and intentionally conspired to commit offenses against the United States, namely:

- a. To knowingly access a computer without authorization and exceed authorized access to a computer, and to obtain thereby information from a protected computer, where the value of the information obtained exceeded \$5,000, in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and 1030(c)(2)(B); and
- b. To knowingly cause the transmission of a program, information, code, and command, and as a result of such conduct, to intentionally cause damage without authorization to a protected computer, and where the offense did cause and, if completed, would have caused, loss aggregating \$5,000 in value to at least one person during a one-year period from a related course of conduct affecting a protected computer, and damage affecting at least ten protected computers during a one-year period, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and 1030(c)(4)(B).

78. In furtherance of the Conspiracy and to effect its illegal objects, OSADCHUK, KOVALEV, and their co-conspirators committed the overt acts set forth in paragraphs 67 through 69 and 71 through 76, which are re-alleged and incorporated by reference as if fully set forth herein.

All in violation of Title 18, United States Code, Section 371.

FORFEITURE ALLEGATION

79. Pursuant to Federal Rule of Criminal Procedure 32.2, notice is hereby given to Defendants that the United States will seek forfeiture as part of any sentence in the event of Defendants' convictions under Counts One, Ten, and Eleven of this Indictment. Pursuant to Title 18, United

States Code, Sections 982(a)(2) and 1030(i), upon conviction of the offenses charged in Counts One and Eleven, Defendants NETYKSHO, ANTONOV, BADIN, YERMAKOV, LUKASHEV, MORGACHEV, KOZACHEK, YERSHOV, MALYSHEV, OSADCHUK, POTEMKIN, and KOVALEV shall forfeit to the United States any property, real or personal, which constitutes or is derived from proceeds obtained directly or indirectly as a result of such violation, and any personal property that was used or intended to be used to commit or to facilitate the commission of such offense. Pursuant to Title 18, United States Code, Section 982(a)(1), upon conviction of the offense charged in Count Ten, Defendants NETYKSHO, ANTONOV, BADIN, YERMAKOV, LUKASHEV, MORGACHEV, KOZACHEK, YERSHOV, MALYSHEV, OSADCHUK, and POTEMKIN shall forfeit to the United States any property, real or personal, involved in such offense, and any property traceable to such property. Notice is further given that, upon conviction, the United States intends to seek a judgment against each Defendant for a sum of money representing the property described in this paragraph, as applicable to each Defendant (to be offset by the forfeiture of any specific property).

Substitute Assets


80. If any of the property described above as being subject to forfeiture, as a result of any act or omission of any Defendant --

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third party;
- c. has been placed beyond the jurisdiction of the court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property that cannot be subdivided without difficulty;

it is the intent of the United States of America, pursuant to Title 18, United States Code, Section

982(b) and Title 28, United States Code, Section 2461(c), incorporating Title 21, United States Code, Section 853, to seek forfeiture of any other property of said Defendant.

Pursuant to 18 U.S.C. §§ 982 and 1030(i); 28 U.S.C. § 2461(c).


Robert S. Mueller, III
Special Counsel
U.S. Department of Justice

A TRUE BILL:

Foreperson

Date: July 13, 2018

FILED

MAY 29 2019

Clerk, U.S. District and
Bankruptcy Courts

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

UNITED STATES OF AMERICA

v.

CONCORD MANAGEMENT &
CONSULTING LLC,

Defendant.

Criminal Action No. 18-cr-32-2 (DLF)

Filed Under Seal

As stated during yesterday's sealed motions hearing, it is

ORDERED that the parties shall abide by Local Criminal Rule 57.7(b) and that the willful failure to do so in the future will result in the initiation of contempt proceedings;

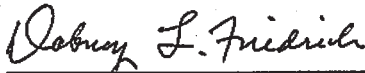
ORDERED that the government shall refrain from making or authorizing any public statement that links the alleged conspiracy in the indictment to the Russian government or its agencies;

ORDERED that to the extent the government makes or authorizes any public statement about the allegations in the indictment, such statement must make clear that (1) the government is summarizing the allegations in the indictment, which remain unproven, and (2) the government does not express an opinion on the defendants' guilt or innocence or the strength of the evidence in this case.

It is further **ORDERED** that the parties shall file supplemental briefs under seal addressing the following questions:

1. Can and should the Court defer consideration of Concord's motion for an order to show cause until after trial, to ensure a fair and impartial trial?
2. If the Court concludes that the government has violated Local Criminal Rule 57.7(b), does the Court have discretion to decline to initiate contempt proceedings and to instead address the violation through alternative means, such as a Rule 57.7(c) order, targeted voir dire questioning, and/or the Court's inherent disciplinary authority?
3. If the Court enters an order regulating the parties' public statements about this case pursuant to Local Criminal Rule 57.7(c), what terms should that order contain? Specifically, how should the Court address the Mueller Report, which has already been disseminated publicly in its current form and which may or may not be disseminated with certain redactions removed, pending the resolution of negotiations between the Department of Justice and Congress and various other court matters?

Both parties shall file their respective memoranda under seal on or before June 5, 2019 and shall file any response to the other party's memorandum under seal on or before June 12, 2019.


DABNEY L. FRIEDRICH
United States District Judge

May 29, 2019

Exhibit I



U.S. Department of Justice

National Security Division

Washington, D.C. 20530

Mr. Ty Clevenger
212 S. Oxford Street. #7D
Brooklyn, NY 112217
Via e-mail to: tyclevenger@yahoo.com

FOI/PA #20-338

16 November 2021

Dear Mr. Clevenger:

This is the National Security Division's (NSD) final response to your Freedom of Information Act (FOIA) request dated June 18, 2020 to the Mail Referral Unit (MRU). The MRU forwarded your request to NSD, and we received your request on June 23, 2020. We have assigned it NSD #20-338.

Specifically, your request states:

1. *I request the opportunity to view all documents, records, communications and/or other tangible evidence reflecting or pertaining to surveillance of Edward Butowsky of Texas or Matt Couch of Arkansas. The term "surveillance" includes, but is not limited to, any attempt to hack into the computers, phones, other electronic devices, and/or online accounts of Mr. Butowsky or Mr. Couch. If any information obtained by surveillance was relayed to third parties, that information should be produced for inspection.*
2. *I request the opportunity to view all documents, records, communications and/or other tangible evidence pertaining to whether former Central Intelligence Agency Director David Petraeus mishandled classified information or sold such information during his tenure as CIA director. This request includes, but is not limited to, documents, records, communications and/or other tangible evidence in the possession of the Office of the Inspector General of the CIA and/or the Office of the Intelligence Community Inspector General. This request further includes, but is not limited to, any draft indictments, draft arrest warrants, actual arrest warrants, and/or records of arrest.*

Regarding item 1 of your request, the NSD, Office of Intelligence represents the government before the Foreign Intelligence Surveillance Court and is responsible for preparing and filing all applications for Court orders pursuant to FISA and maintains files documenting those applications and orders. Because confirming or denying whether records responsive to

FOIA requests exist would disclose information exempt from disclosure under FOIA, we do not search these records in response to FOIA requests. Any such information is properly classified under Executive Order 13526. To confirm or deny the existence of such records in each case would reveal properly classified information regarding intelligence sources and methods. Accordingly, we can neither confirm nor deny the existence of records in these files responsive to your request pursuant to 5 U.S.C. 552(b)(1).

Regarding item 2 of your request, a search of the Counterintelligence and Export Control Section of NSD was conducted. We located records responsive to your request. We are releasing them in full. Copies are attached. We also located a record which originated in the Office of the United States Attorney for the Eastern District of Virginia. We have referred that record to the Executive Office for United States Attorneys for review and direct response to you.

As this matter is already in litigation, we are omitting our standard appeal paragraph. If you have any questions concerning this response please contact Assistant United States Attorney, Andrea Parker of the Eastern District of Texas at (409) 839-2538.

Sincerely,

A handwritten signature in blue ink, appearing to read "Kevin G. Tiernan".

Kevin G. Tiernan
Records and FOIA

Enclosures

FILED
CHARLOTTE, NC

MAR 3 2015

U.S. DISTRICT COURT
WESTERN DISTRICT OF NC

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION

UNITED STATES OF AMERICA)
)
 v.)
)
 DAVID HOWELL PETRAEUS)
)

DOCKET NO. 3:15 CR 47

FACTUAL BASIS

NOW COMES the United States of America, by and through Anne M. Tompkins, United States Attorney for the Western District of North Carolina, James P. Melendres, Trial Attorney, Jill Westmoreland Rose, Assistant United States Attorney, and Richard S. Scott, Trial Attorney, and hereby files this Factual Basis in support of the Plea Agreement filed simultaneously in this matter.

This Factual Basis does not attempt to set forth all of the facts known to the United States at this time. By their signatures below, the parties expressly agree that there is a factual basis for the guilty plea that the defendant will tender pursuant to the Plea Agreement. The parties also agree that this Factual Basis may, but need not, be used by the United States Probation Office and the Court in determining the applicable advisory guideline range under the United States Sentencing Guidelines or the appropriate sentence under 18 U.S.C. § 3553(a). The defendant agrees not to object to any fact set forth below being used by the Court or the United States Probation Office to determine the applicable advisory guideline range or the appropriate sentence under 18 U.S.C. § 3553(a). The parties' agreement does not preclude either party from hereafter presenting the Court with additional facts which do not contradict facts to which the parties have agreed not to object and which are relevant to the Court's guideline computations, to 18 U.S.C. § 3553 factors, or to the Court's overall sentencing decision.

The parties stipulate that the allegations in the Bill of Information and the following facts are true and correct, and that had the matter gone to trial, the United States would have proven them beyond a reasonable doubt with admissible and credible evidence. Specifically, the evidence would establish, at a minimum, the following facts:

At all relevant times,

The Defendant

1. Defendant DAVID HOWELL PETRAEUS, a citizen of the United States and resident of Arlington, Virginia, was a United States Army four-star general when he retired from the Army on or about August 31, 2011. From on or about July 4, 2010, to on or about July 18, 2011, defendant DAVID HOWELL PETRAEUS served as Commander of the International Security Assistance Force (“ISAF”) in Afghanistan. From on or about September 6, 2011, to on or about November 9, 2012, defendant DAVID HOWELL PETRAEUS served as Director of the Central Intelligence Agency (“CIA”).

Classified Information

2. Those persons with security clearances granting them access to classified information were required to properly store and secure classified information, by Title 18, United States Code, Sections 793 and 1924, and applicable rules, regulations, and orders.

3. Classified information was defined by Executive Order 13526 (“E.O. 13526”) and relevant preceding Executive Orders, as information in any form that: (1) is owned by, produced by or for, or under the control of the United States government; (2) falls within one or more of the categories set forth in E.O. 13526; and (3) is classified by an original classification authority

who determines that its unauthorized disclosure reasonably could be expected to result in damage to the national security. Where such unauthorized disclosure reasonably could be expected to cause “damage” to the national security, the information is classified as “Confidential.” Where such unauthorized disclosure reasonably could be expected to cause “serious damage” to the national security, the information is classified as “Secret.” Where such unauthorized disclosure reasonably could be expected to cause “exceptionally grave damage” to the national security, the information is classified as “Top Secret.”

4. E.O. 13526 also provides that certain senior U.S. officials are authorized to establish “special access programs” upon a finding that “the vulnerability of, or threat to, specific information is exceptional” and “the normal criteria for determining eligibility for access applicable to information classified at the same level are not deemed sufficient to protect the information from unauthorized disclosure.” Within the U.S. Intelligence Community, the Director of National Intelligence is authorized to establish special access programs for intelligence sources, methods, and activities. Such intelligence programs are called “Sensitive Compartmented Information Programs” or SCI Programs. A term commonly used to describe certain materials in such programs is “code word.”

5. Pursuant to E.O. 13526, a person may gain access to classified information only if a favorable determination of eligibility for access has been made by an agency head or an agency head’s designee, the person has signed an approved nondisclosure agreement, and the person has a “need-to-know” the information.

6. “Need-to-know” means a determination by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized government function.

7. The classified information being accessed may not be removed from the controlling agency’s premises without permission. Moreover, even when SCI is maintained on the controlling agency’s premises, it must be stored in a Sensitive Compartmented Information Facility (“SCIF”), which is an accredited area, room, group of rooms, building, or installation designed to prevent as well as detect visual, acoustical, technical, and physical access by unauthorized persons.

The Department of Defense

8. The Department of Defense (“DOD”) was a United States government military agency. The DOD’s headquarters were at Arlington, Virginia. The DOD was responsible for providing the military forces needed to deter war and protect the security of the United States. Moreover, through its subordinate national intelligence services, including the Defense Intelligence Agency, the National Security Agency, the National Geospatial-Intelligence Agency, and the National Reconnaissance Office, the DOD was responsible for, among other things, collecting information that revealed the military plans, intentions, and capabilities of the United States’ adversaries and the bases for their decisions and actions, as well as conducting clandestine actions, at the direction of the President and his authorized designee, designed to preempt threats and achieve the United States’ policy objectives.

9. The responsibilities of certain DOD employees required that their association with the DOD be kept secret; as a result, the fact that these individuals were employed by the DOD

was classified. The responsibilities of other DOD employees required that, while their employment by the DOD was itself not secret, their association with certain DOD programs and their particular activities on behalf of the DOD were kept secret; accordingly, such information was classified. Disclosure of the fact that such individuals were employed by the DOD, associated with certain DOD programs, or engaged in particular activities on behalf of the DOD, had the potential to damage national security in ways that ranged from preventing the future use of individuals in a covert or clandestine capacity, to compromising clandestine actions and intelligence-gathering methods and operations, to endangering the safety of DOD employees and those who interacted with them.

The Central Intelligence Agency

10. The CIA was a United States government intelligence agency. The CIA's headquarters were at Langley, Virginia. The CIA was responsible for, among other things, collecting information that revealed the plans, intentions, and capabilities of the United States' adversaries and the bases for their decisions and actions, as well as conducting clandestine actions, at the direction of the President and his authorized designees, designed to preempt threats and achieve the United States' policy objectives.

11. The responsibilities of certain CIA employees required that their association with the CIA be kept secret; as a result, the fact that these individuals were employed by the CIA was classified. The responsibilities of other CIA employees required that, while their employment by the CIA was itself not necessarily secret, their association with certain CIA programs and their particular activities on behalf of the CIA be kept secret; accordingly, such information was classified. Disclosure of the fact that such individuals were employed by the CIA, associated

with certain CIA programs, or engaged in particular activities on behalf of the CIA, had the potential to damage national security in ways that ranged from preventing the future use of individuals in a covert or clandestine capacity, to compromising clandestine actions and intelligence-gathering methods and operations, to endangering the safety of CIA employees and those who dealt with them.

Criminal Conduct

12. Throughout his employment by the DOD, defendant DAVID HOWELL PETRAEUS entered into various agreements with the United States regarding the protection and proper handling of classified information. Examples of these agreements include:

a. On March 15, 2006, as a condition of being granted access to certain SCI, DAVID HOWELL PETRAEUS entered into a Non-Disclosure Agreement (“NDA”) with the DOD in which he agreed, in pertinent part, as follows:

I have been advised that unauthorized disclosure, unauthorized retention, or negligent handling of SCI by me could cause irreparable injury to the United States or be used to advantage by a foreign nation. I hereby agree that I will never divulge anything marked as SCI or that I know to be SCI to anyone who is not authorized to receive it without prior written authorization from the United States Government department or agency . . . that last authorized my access to SCI.

I hereby agree to submit for security review by the [agency] that last authorized my access to such information or material, any writing or other preparation in any form . . . that contains or purports to contain any SCI . . . that I contemplate disclosing to any person not authorized to have access to SCI . . .

In addition, I have been advised that any unauthorized disclosure of SCI by me may constitute a violation or violations of United States criminal laws, including the provisions of . . . Section[] 793 . . . [of] Title 18, United States Code . . .

I agree that I shall return all materials that may have come into my possession or for which I am responsible because of such access, upon demand by an authorized representative of the United States Government or upon the conclusion of my employment or other relationship with the United States Government entity

providing me access to such materials. If I do not return such materials upon request, I understand this may be a violation of Section 793, Title 18, United States Code . . .

Defendant DAVID HOWELL PETRAEUS entered into at least 13 additional NDAs in the course of his DOD employment. In each instance, DAVID HOWELL PETRAEUS promised never to disclose SCI to anyone not authorized to receive it without prior written authorization from the United States government, and he acknowledged that unauthorized retention and/or disclosure of classified information could cause irreparable injury to the United States and be used to advantage by a foreign nation. The scope of these NDAs encompassed classified information referenced in this Statement of Facts.

b. As a condition of being granted access to classified information, defendant DAVID HOWELL PETRAEUS entered into a Secrecy Agreement with the DOD, in which he agreed, in pertinent part, as follows:

I accept the responsibilities associated with being granted access to classified national security information. I am aware of my obligation to protect classified national security information through proper safeguarding and limiting access to individuals with the proper security clearance and official need to know. I further understand that, in being granted access to classified information, a special confidence and trust has been placed in me by the United States Government.

Defendant DAVID HOWELL PETRAEUS entered into at least 13 additional Secrecy Agreements in the course of his DOD employment. In each instance, defendant DAVID HOWELL PETRAEUS agreed to protect classified national security information through proper safeguarding and limiting access to individuals with proper security clearance and official need-to-know.

13. On or about August 31, 2011, defendant DAVID HOWELL PETRAEUS retired from the DOD, after which time he retained his continuing lifelong obligation to the United

States to protect the classified information to which he had been granted access while employed by the DOD.

14. As a condition of his employment by the CIA, defendant DAVID HOWELL PETRAEUS entered into various agreements with the United States, including, for example, the following:

a. On June 16, 2011, as a condition of being granted access to certain SCI, defendant DAVID HOWELL PETRAEUS entered into a NDA with the CIA which was materially identical to the March 2006 NDA he signed while employed by the DOD.

b. On November 26, 2012, following his resignation from the CIA, defendant DAVID HOWELL PETRAEUS entered into a Secrecy Agreement with the CIA in which he agreed, in pertinent part, as follows:

I understand that in the course of my employment . . . I may be given access to information or material that is classified or is in the process of a classification determination . . . that, if disclosed in an unauthorized manner would jeopardize intelligence activities of the United States Government. I accept that by being granted access to such information or material I will be placed in a position of special confidence and trust and become obligated to protect the information and/or material from unauthorized disclosure.

As a further condition of the special confidence and trust reposed in me by the Central Intelligence Agency, I hereby agree to submit for review by the Central Intelligence Agency any writing or other preparation in any form . . . which contains any mention of intelligence data or activities, or contains any other information or material that might be based on [classified information] . . .

I understand that . . . the disclosure of information that I agreed herein not to disclose can, in some circumstances, constitute a criminal offense . . .

15. On or about November 9, 2012, defendant DAVID HOWELL PETRAEUS resigned from the CIA, after which time he retained his continuing lifelong obligation to the

United States to protect the classified information to which he had been granted access while employed by the CIA.

16. During his tenure at the DOD and the CIA, defendant DAVID HOWELL PETRAEUS held a United States government security clearance allowing him access to classified United States government information. As a result, defendant DAVID HOWELL PETRAEUS had regular access to classified and national defense information relating to DOD and CIA programs, operations, methods, sources, and personnel.

17. During his tenure as Commander of ISAF in Afghanistan, defendant DAVID HOWELL PETRAEUS maintained bound, five-by-eight-inch notebooks that contained his daily schedule and classified and unclassified notes he took during official meetings, conferences, and briefings. The notebooks had black covers and, for identification purposes, defendant DAVID HOWELL PETRAEUS taped his business card on the front exterior of each notebook. A total of eight such books (hereinafter the "Black Books") encompassed the period of defendant DAVID HOWELL PETRAEUS's ISAF Command and collectively contained classified information regarding the identities of covert officers, war strategy, intelligence capabilities and mechanisms, diplomatic discussions, quotes and deliberative discussions from high-level National Security Council meetings, and defendant DAVID HOWELL PETRAEUS's discussions with the President of the United States of America.

18. The Black Books contained national defense information, including Top Secret//SCI and code word information.

19. The National Defense University ("NDU") was an institution of higher education funded by the DOD, intended to facilitate high-level training and education, as well as the

development of national security strategy. It was located on the grounds of Fort Lesley McNair, in Washington, D.C. NDU was a repository for the DOD's classified collections.

20. From in or about July 2009 to in or about July 2012, defendant DAVID HOWELL PETRAEUS's DOD historian gathered and organized the classified materials that defendant DAVID HOWELL PETRAEUS collected during his DOD tenure. Defendant DAVID HOWELL PETRAEUS never provided the Black Books to his DOD historian. Instead, defendant DAVID HOWELL PETRAEUS personally retained the Black Books.

21. In or about September 2012, defendant DAVID HOWELL PETRAEUS's DOD historian transferred defendant DAVID HOWELL PETRAEUS's classified collection to NDU for storage and archiving. Because defendant DAVID HOWELL PETRAEUS personally retained the Black Books, they were never transferred to NDU.

22. On or about August 4, 2011, after defendant DAVID HOWELL PETRAEUS returned permanently to the United States from Afghanistan, during a conversation, recorded by his biographer, defendant DAVID HOWELL PETRAEUS stated that the Black Books were "highly classified" and contained "code word" information:

Biographer:	By the way, where are your black books? We never went through, . . .
PETRAEUS:	They're in a rucksack up there somewhere.
Biographer:	Okay . . . You avoiding that? You gonna look through 'em first?
PETRAEUS:	Umm, well, they're really -- I mean they are highly classified, some of them. They don't have it on it, but I mean there's code word stuff in there.

23. On or about August 27, 2011, defendant DAVID HOWELL PETRAEUS sent an e-mail to his biographer in which he agreed to provide the Black Books to his biographer.

24. On or about August 28, 2011, defendant DAVID HOWELL PETRAEUS delivered the Black Books to a private residence in Washington, D.C. (the “DC Private Residence”), where his biographer was staying during a week-long trip to Washington, D.C. The DC Private Residence was not approved for the storage of classified information.

25. Thereafter, from on or about August 28, 2011, to on or about September 1, 2011, defendant DAVID HOWELL PETRAEUS left the Black Books at the DC Private Residence in order to facilitate his biographer’s access to the Black Books and the information contained therein to be used as source material for his biography, titled *All In: The Education of General David Petraeus*, released by Penguin Press in 2012. No classified information from the Black Books appeared in the aforementioned biography.

26. On or about September 1, 2011, defendant DAVID HOWELL PETRAEUS retrieved the Black Books from the DC Private Residence and returned them to his own Arlington, Virginia home (the “PETRAEUS Residence”).

27. On or about November 9, 2012, defendant DAVID HOWELL PETRAEUS resigned from the CIA. Approximately two weeks after his November 9, 2012 resignation, defendant DAVID HOWELL PETRAEUS was debriefed and read-out of the SCI compartments and Special Access Programs to which he previously had been granted access. Specifically, on or about November 26, 2012, defendant DAVID HOWELL PETRAEUS executed two SCI NDAs which contained debriefing acknowledgments, a Secrecy Agreement, and a Security Exit Form. The Security Exit Form included seven provisions regarding his continuing duty to

protect classified information from disclosure. Among other things, by signing the Security Exit Form, defendant DAVID HOWELL PETRAEUS adopted the following provision: "I give my assurance that there is no classified material in my possession, custody, or control at this time." At the time he provided this assurance, the Black Books were still in the PETRAEUS Residence.

28. On or about January 3, 2013, a SCIF, which had been installed at the PETRAEUS Residence by the CIA during defendant DAVID HOWELL PETRAEUS's tenure as CIA Director, was closed and de-accredited. The SCIF was subsequently removed on or about February 13, 2013.

29. On or about April 5, 2013, the FBI executed a court-authorized search warrant at the PETRAEUS Residence and seized the Black Books from an unlocked desk drawer in the first-floor study of the PETRAEUS Residence.

30. Between in or about August 2011, and on or about April 5, 2013, defendant DAVID HOWELL PETRAEUS, being an employee of the United States, and by virtue of his employment, became possessed of documents and materials containing classified information of the United States, and did unlawfully and knowingly remove such documents and materials without authority and thereafter intentionally retained such documents and materials at the DC Private Residence and the PETRAEUS Residence, aware that these locations were unauthorized for the storage and retention of such classified documents and materials.

31. On or about June 12, 2012, in two separate interviews conducted by special agents of the Federal Bureau of Investigation ("FBI") regarding investigations unrelated to the instant offense, defendant DAVID HOWELL PETRAEUS acknowledged that he understood that making false statements to the FBI in the course of a criminal investigation was a crime.

Specifically, on June 12, 2012, defendant DAVID HOWELL PETRAEUS was interviewed in his office at CIA Headquarters in Langley, Virginia, in connection with two media leak investigations. During both interviews, defendant DAVID HOWELL PETRAEUS affirmed in writing, "I understand that providing false statements to the Federal Bureau of Investigation is a violation of law."

32. On or about October 26, 2012, defendant DAVID HOWELL PETRAEUS was interviewed by two FBI special agents in his office at CIA Headquarters in Langley, Virginia. Defendant DAVID HOWELL PETRAEUS was advised that the special agents were conducting a criminal investigation. During that interview, the special agents questioned DAVID HOWELL PETRAEUS about the mishandling of classified information. In response to those questions, defendant DAVID HOWELL PETRAEUS stated that (a) he had never provided any classified information to his biographer, and (b) he had never facilitated the provision of classified information to his biographer. These statements were false. Defendant DAVID HOWELL PETRAEUS then and there knew that he previously shared the Black Books with his biographer.

33. The acts taken by defendant DAVID HOWELL PETRAEUS were in all respects knowing and deliberate, and were not committed by mistake, accident, or other innocent reason.

34. This Statement of Facts includes those facts necessary to support the Plea Agreement between the defendant and the government. It does not include each and every fact known to the defendant or to the government, and it is not intended to be a full enumeration of all the facts surrounding defendant DAVID HOWELL PETRAEUS's case.

//

//

United States Sentencing Guidelines

35. Further, in accordance with Fed. R. Crim. P. 11(c)(1)(B) of the Federal Rules of Criminal Procedure, the United States and the defendant will recommend to the Court that the following provisions of the United States Sentencing Guidelines apply:

Base Offense Level:	6	[U.S.S.G. § 2X5.2]
Abuse of Position of Trust:	+2	[U.S.S.G. § 3B1.3]
Obstruction of Justice	+2	[U.S.S.G. § 3C1.1]
Acceptance of Responsibility	-2	[U.S.S.G. § 3E1.1(a)]
Total Adjusted Offense Level	8	

ANNE M. TOMPKINS
UNITED STATES ATTORNEY


JAMES P. MELENDRES
TRIAL ATTORNEY


JILL WESTMORELAND ROSE
ASSISTANT UNITED STATES ATTORNEY


RICHARD S. SCOTT
TRIAL ATTORNEY

2/23/2015

Feb. 23, 2015

2/23/2015

//

//


//

//

//

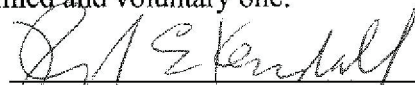
Defendant's Signature: After consulting with my attorney, and pursuant to the Plea Agreement entered into this day between myself and the United States, I hereby stipulate that the above Factual Basis is true and accurate, and that had the matter proceeded to trial, the United States would have proved the same beyond a reasonable doubt.

Date: 22 February 2015


David Howell Petraeus
Defendant

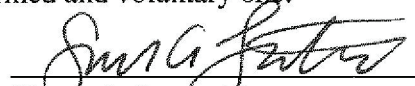
Defense Counsel Signature: I am counsel for the defendant in this case. I carefully reviewed the above Factual Basis with the defendant. To my knowledge, the defendant's decision to stipulate to these facts is an informed and voluntary one.

Date: Feb 23, 2015


David E. Kendall
Williams & Connolly LLP
Counsel for the Defendant

Defense Counsel Signature: I am counsel for the defendant in this case. I carefully reviewed the above Factual Basis with the defendant. To my knowledge, the defendant's decision to stipulate to these facts is an informed and voluntary one.

Date: Feb. 23, 2015


Simon A. Latcoyich
Williams & Connolly LLP
Counsel for the Defendant

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION

FILED
CHARLOTTE, NC
MAR 3 2015

U.S. DISTRICT COURT
WESTERN DISTRICT OF NC

UNITED STATES OF AMERICA

v.

DAVID HOWELL PETRAEUS

) DOCKET NO.: 3:15 CR 47

) PLEA AGREEMENT

NOW COMES the United States of America, by and through Anne M. Tompkins, United States Attorney for the Western District of North Carolina, James P. Melendres, Trial Attorney, Jill Westmoreland Rose, Assistant United States Attorney, and Richard S. Scott, Trial Attorney, the defendant, David Howell Petraeus, and the defendant's counsel, David E. Kendall and Simon A Latcovich, and respectfully inform the Court that they have reached an agreement pursuant to Federal Rule of Criminal Procedure 11. References to the United States herein shall mean the United States Attorney for the Western District of North Carolina.

I. Plea

1. The defendant agrees to enter a voluntary plea of guilty to Count ONE as set forth in the Bill of Information, and admits to being in fact guilty as charged in Count ONE.

2. The defendant understands that each and every provision set forth below is a material term of the Plea Agreement. The defendant's failure to fully comply with any provision of the Plea Agreement, attempt to withdraw the guilty plea or violation of any federal, state, or local law, or any order of any court, including any condition of pre-trial or pre-sentence, or post-sentence release is a breach of the Plea Agreement. In addition to any other remedy available in law, the defendant's breach (i) will relieve the United States of its obligations under the Plea Agreement, but the defendant will not be relieved of the defendant's obligations or allowed to withdraw the guilty plea; (ii) may constitute the defendant's failure to accept responsibility under United States Sentencing Guideline ("U.S.S.G.") § 3E1.1; and (iii) will permit the United States to proceed on any dismissed, pending, superseding, or additional charges.

II. Venue Waiver

3. The United States and the defendant agree and stipulate that this District is an appropriate venue for entry of a plea by the defendant to a Bill of Information charging a violation of 18 U.S.C. § 1924.

III. Sentence

4. The defendant is aware that the statutory maximum sentence for Count ONE is as follows:

Count ONE: a violation of 18 U.S.C. § 1924; a maximum term of one year imprisonment, a \$100,000 fine, or both, a special assessment of \$25, and no more than 5 years of probation.

5. The defendant understands that a violation of any terms or conditions of supervised release, should it be imposed, may subject the defendant to an additional period of incarceration.

6. The defendant is aware that the Court: (a) will consider the advisory U.S.S.G. in determining the sentence; (b) has not yet determined the sentence and any estimate of the likely sentence is a prediction rather than a promise; (c) has the final discretion to impose any sentence up to the statutory maximum; and (d) is not bound by recommendations or agreements by the United States. Knowing this, the defendant understands that the defendant may not withdraw the plea as a result of the sentence imposed.

7. Pursuant to Fed. R. Crim. P. 11(c)(1)(B), the parties agree that they will jointly recommend that the Court make the following findings and conclusions as to the U.S.S.G:

a. The offense level for the subject offense is as follows:

Base Offense Level:	6	[U.S.S.G. § 2X5.2]
Abuse of Position of Trust:	+2	[U.S.S.G. § 3B1.3]
Obstruction of Justice	+2	[U.S.S.G. § 3C1.1]
Acceptance of Responsibility	-2	[U.S.S.G. § 3E1.1]
Total Adjusted Offense Level	8	

b. Unless otherwise set forth herein, the parties agree that they will make the above recommendations as to the adjusted offense level, and will recommend no other enhancements or reductions to the Court.

8. The United States agrees not to oppose the defendant's request that the defendant receive a non-custodial sentence.

9. The parties jointly recommend the imposition of a two-year term of probation.

10. The parties jointly recommend the imposition of a \$40,000 fine.

11. The parties jointly waive the preparation of a Pre-Sentence Report. However, the defendant expressly acknowledges that the Court is not bound by this waiver and recommendation. The parties will inform the Court and the United States Probation Office of all facts pertinent to the sentencing process and will present any evidence requested by the Court.

12. The defendant agrees to the following with respect to financial disclosures, monetary penalties, forfeiture, and restitution:

a. To make full payment of such fine as the Court may impose, within one week of the sentencing hearing. If such full payment is not made within one week of sentencing hearing, to make full disclosure of all current and projected assets to the U.S. Probation Office immediately and prior to the termination of the defendant's supervised release or probation, such disclosures to be shared with the U.S. Attorney's Office, including the Financial Litigation Unit, for any purpose.

b. That monetary penalties imposed by the Court will be (i) subject to immediate enforcement as provided for in 18 U.S.C. § 3613, and (ii) submitted to the Treasury Offset Program so that any federal payment or transfer of returned property the defendant receives may be offset and applied to federal debts but will not affect the periodic payment schedule.

IV. Immunity from Further Prosecution in This District and Others

13. The United States will not bring any additional criminal charges against the defendant for the conduct outlined in the Factual Basis or for any other criminal offenses committed by the defendant which are known to the United States at the time of disposition.

V. Procedure

14. The defendant will plead guilty because the defendant is in fact guilty of the charged offense. The defendant admits the facts set forth in the Factual Basis filed with this Plea Agreement and agrees that those facts establish guilt of the offense charged beyond a reasonable doubt. The Factual Basis, which is hereby incorporated into this Plea Agreement, constitutes a stipulation of facts for purposes of § 1B1.2(a) of the U.S.S.G. and Fed. R. Crim. P. 11(b)(3).

15. The defendant further stipulates that the Factual Basis may be used by the Court and the United States Probation Office without objection by the defendant to determine the applicable advisory guideline range or the appropriate sentence under 18 U.S.C. § 3553(a).

VI. Waivers

16. The defendant is aware that the law provides certain limited rights to withdraw a plea of guilty, has discussed these rights with defense counsel and knowingly and expressly waives any right to withdraw the plea once the Court has accepted it.

17. The defendant acknowledges that Fed. R. Crim. P. 11(f) and Fed. R. of Evid. 408 and 410 are rules which ordinarily limit the admissibility of statements made by a defendant in the course of plea discussions. The defendant knowingly and voluntarily waives these rights and

agrees that any statements made in the course of the defendant's guilty plea or this Plea Agreement (in part or in its entirety, at the sole discretion of the United States) will be admissible against the defendant for any purpose in any criminal or civil proceeding if the defendant fails to enter or attempts to withdraw the defendant's guilty plea, or in any post-conviction proceeding challenges the voluntary nature of the guilty plea.

18. The defendant agrees that by pleading guilty, the defendant is expressly waiving the right: (a) to be tried by a jury; (b) to be assisted by an attorney at trial; (c) to confront and cross-examine witnesses; and (d) not to be compelled to incriminate himself.

19. The defendant has discussed with his attorney: (1) defendant's rights pursuant to 18 U.S.C. § 3742, 28 U.S.C. § 2255, and similar authorities to contest a conviction and/or sentence through an appeal or post-conviction after entering into a Plea Agreement; (2) whether there are potential issues relevant to an appeal or post-conviction action; and (3) the possible impact of any such issue on the desirability of entering into this Plea Agreement.

20. The defendant, in exchange for the concessions made by the United States in this Plea Agreement, waives all such rights to contest the conviction except for: (1) claims of ineffective assistance of counsel or (2) prosecutorial misconduct. The defendant also knowingly and expressly waives all rights conferred by 18 U.S.C. § 3742 or otherwise to appeal whatever sentence is imposed with the two exceptions set forth above. The defendant agrees that the United States preserves all its rights and duties as set forth in 18 U.S.C. § 3742(b).

21. The defendant waives all rights, whether asserted directly or by a representative, to request or to receive from any department or agency any records pertaining to the investigation or prosecution of this case, including without limitation any records that may be sought under the Freedom of Information Act, 5 U.S.C. § 552, or the Privacy Act, 5 U.S.C. § 552a.

VII. Conclusion

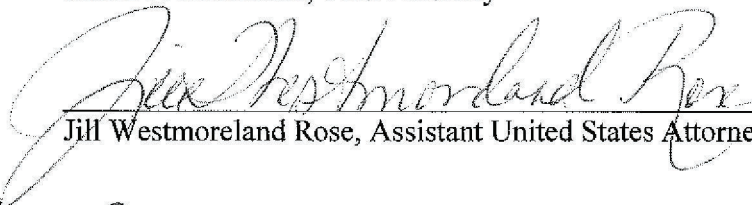
22. This agreement is effective and binding once signed by the defendant, the defendant's attorney, and an attorney for the United States. The defendant agrees to entry of this Plea Agreement at the date and time scheduled by the Court.

23. There are no agreements, representations, or understandings between the parties in this case, other than those explicitly set forth in this Plea Agreement, or as noticed to the Court during the plea colloquy and contained in writing in a separate document signed by all parties.

SO AGREED:


James P. Melendres, Trial Attorney


DATED: 2/23/2015


Jill Westmoreland Rose, Assistant United States Attorney

DATED: Feb. 23, 2015


Richard S. Scott, Trial Attorney


DATED: 2/23/2015


David E. Kendall, Attorney for Defendant
Williams & Connolly LLP

DATED: Feb 23, 2015


Simon A. Latcovich, Attorney for Defendant
Williams & Connolly LLP

DATED: Feb. 23, 2015


David Howell Petraeus, Defendant

DATED: 22 February 2015

Revised January 2015